REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b. OFFICE SYMBOL (*If applicable*) 55	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000	7b ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (*If applicable*)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (*City, State, and ZIP Code*)	10 SOURCE OF FUNDING NUMBERS Program Element No / Project No / Task No / Work Unit Accession Number

11 TITLE (*Include Security Classification*)
C3 Interoperability Issues: An Overview of GOSIP Network Conformance Testing in the Evolution of the Defense Systems Information Network (DISN)

12 PERSONAL AUTHOR(S) Wayne R. Martin

13a. TYPE OF REPORT	13b. TIME COVERED	14 DATE OF REPORT (*year, month, day*)	15 PAGE COUNT
Master's Thesis	From To	June 1992	191

16. SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 COSATI CODES			18 SUBJECT TERMS (*continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	GOSIP Conformance Testing, DISN, ISDN, B-ISDN, Interoperability, C3 MILDEP Network Architectures, Open Systems.

19 ABSTRACT (*continue on reverse if necessary and identify by block number*)

This thesis analyzes some of the evolving commercial-off-the-shelf (COTS) technologies and potential difficulties in implementing the proposed Defense Information System Network (DISN) based on Government Open Systems Interconnection Profile (GOSIP) compliance and Integrated Services Digital Network (ISDN) conformance testing. It starts by examining the MILDEPs Command, Control, and Communications (C3) network architectures by providing brief descriptions of the various standards. Not only does it examine such technologies as Fiber Distributed Data Interface (FDDI), Synchronous Optical Network (SONET), Fast Packet Switching (FPS), and Broadband ISDN, but it also highlights some of the ISDN conformance test suites with a view toward migrating these architectures and technologies to the DISN. Results indicate that incompatibilities between C3 networks will be impacted more in the DISN near-term and transition phases than in the far-term. This is due in part to embedded proprietary functions permeating COTS products and the lack of fully developed ISDN conformance test specifications. The lack of clearly defined standards is a major cause of proprietary implementations. Coupled with the limited availability of ISDN conformance test suites to test multi-vendored MILDEP C3 networks, this will make deployment of the DISN a challenge. Recommendations for further research are also presented.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED	
22a. NAME OF RESPONSIBLE INDIVIDUAL Myung Suh	22b TELEPHONE (*Include Area code*) (408) 646-2637	22c OFFICE SYMBOL AS/SU

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

Approved for public release; distribution is unlimited.

C3 INTEROPERABILITY ISSUES: AN OVERVIEW OF GOSIP NETWORK CONFORMANCE TESTING IN THE EVOLUTION OF THE DEFENSE INFORMATION SYSTEM NETWORK (DISN)

by

Wayne R. Martin
Captain, United States Air Force
B.S., Troy State University, 1981

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

ABSTRACT

This thesis analyzes some of the evolving commercial-off-the-shelf (COTS) technologies and potential difficulties in implementing the proposed Defense Information System Network (DISN) based on Government Open Systems Interconnection Profile (GOSIP) compliance and Integrated Services Digital Network (ISDN) conformance testing. It starts by examining the MILDEPs Command, Control, and Communications (C^3) network architectures by providing brief descriptions of the various standards. Not only does it examine such technologies as Fiber Distributed Data Interface (FDDI), Synchronous Optical Network (SONET), Fast Packet Switching (FPS), and Broadband ISDN, but it also highlights some of the ISDN conformance test suites with a view toward migrating these architectures and technologies to the DISN. Results indicate that incompatibilities between C^3 networks will be impacted more in the DISN near-term and transition phases than in the far-term. This is due in part to embedded proprietary functions permeating COTS products and the lack of fully developed ISDN conformance test specifications. The lack of clearly defined standards is a major cause of proprietary implementations. Coupled with the limited availability of ISDN conformance test suites to test multi-vendored MILDEP C^3 networks, this will make deployment of the DISN a challenge. Recommendations for further research are also presented.

1 10513
M3589
C.1

TABLE OF CONTENTS

I. INTRODUCTION 1

A. BACKGROUND 1

B. PROBLEM 3

C. GUIDE TO THE FOLLOWING CHAPTERS 5

II. C^3 SYSTEMS ARCHITECTURE 7

A. BACKGROUND 7

B. EVOLUTION OF THE DEFENSE INFORMATION SYSTEMS NETWORK (DISN) 8

1. Background 8

2. Existing DoD Network Architecture 9

3. Technology Considerations 10

4. DISN Phased Development 12

C. MILITARY DEPARTMENT ARCHITECTURES 19

1. Air Force Information Transfer Architecture (ITA) 19

2. Navy Copernicus Architecture 25

3. Army Information System Architecture (ISA) 32

III. GOVERNMENT OPEN SYSTEMS INTERCONNECTION PROFILE (GOSIP) 38

A. DEVELOPMENT OF OSI AND GOSIP 38

1. Background 38

2. Concept 39

3. Objective 42

4. Applicability 42

B. OSI ARCHITECTURE AND STANDARDS 44

C. DEPARTMENT OF DEFENSE (DoD) PROTOCOL MODEL AND MIGRATION TO GOSIP 45

1. DoD Protocols 47

2. Transition Strategy 51

D. GOSIP MAJOR SUBNETWORK TECHNOLOGIES 53

1. CSMA/CD Bus (8802/3) 53

2. Token Bus (8802/4) 54

3. Token Ring (8802/5) 55

4. X.25 Wide Area Networks (WANs) 56

5. Integrated Services Digital Network (ISDN) 56

6. Local Area Network Bridges 57

E. END-TO-END PROTOCOL CONSIDERATIONS 58

1. Transport Layer 58

2. Network Layer 60

F. GOSIP SECURITY CONSIDERATIONS 61

G. FUTURE GOSIP RELEASE VERSIONS 65

IV. DATA SERVICES USING INTEGRATED SERVICES DIGITAL NETWORK (ISDN) 67

A. ISDN CONCEPT AND OBJECTIVE 68

B. ISDN RELATIONSHIP TO OSI 71

C. ISDN STANDARDS AND FEATURES 73

1. Bearer Services and Teleservices 74

2. Physical Layer Standards 76

3. Data Link Layer and Services 84

4. Network Layer and Services (Q.931/I.451) 88

D. DoD ISDN PROFILES 98

1. Mandatory Profiles 98

2. Optional Profiles 99

E. PROPOSED ISDN FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 100

F. NATIONAL INTEGRATED SERVICES DIGITAL NETWORK (NATIONAL ISDN) 101

G. SUMMARY 102

V. OVERVIEW OF BROADBAND ISDN (B-ISDN) AND OTHER DIGITAL TECHNOLOGIES 104

A. BROADBAND-ISDN 104

1. Background, Concept and Objective 104

2. Asynchronous Transfer Mode (ATM) and Characteristics 106

3. Current Direction of B-ISDN 109

4. Future Direction of B-ISDN 110

B. OTHER DIGITAL TECHNOLOGIES 111

1. Frame Relay 111

2. Switch Multi-Megabit Data Service (SMDS) 113

3. Fiber Distributed Data Interface (FDDI) 115

4. Synchronous Optical Network (SONET) 116

C. SUMMARY 119

VI. CONFORMANCE GUIDELINES AND TEST PROCEDURES 120

A. BACKGROUND 120

B. ORGANIZATIONS ESTABLISHING TEST POLICY 121

1. National Institute of Standards and Technology (NIST) 121

2. North American ISDN Users' Forum (NIU-Forum) 122

3. Corporation for Open System (COS) International 122

C. TESTING LABORATORIES 123

1. NIST Computer Systems Laboratory (CSL) 124

2. COS Conformance Test Laboratory 125
3. DoD Joint Interoperability Test Center (JITC) 125
4. MILDEP Testing Programs 127
D. CONFORMANCE TESTING AND PROCESS 129
1. Description of Conformance Testing 131
2. Abstract and Executable Test Suites 132
3. Protocol Implementation Conformance Statement (PICS) 133
4. Protocol Conformance Test Report (PCTR) 135
5. System Conformance Test Statement Report (SCTR) 136
E. CONFORMANCE TEST SUITES 137
1. Physical Layer Test Specifications 137
2. Data Link Layer Test Specifications 138
3. Network Layer Test Specifications 139
F. DoD ISDN CONFORMANCE TESTING 139
G. BEYOND CONFORMANCE TESTING 141
1. Interoperability Testing 142
2. Performance Testing 142
3. Functional Testing 144
H. SUMMARY 145

VII. SUMMARY AND CONCLUSIONS 147
A. SUMMARY 147

B. CONCLUSIONS 149

C. AREAS RECOMMENDED FOR FURTHER RESEARCH 150

1. Federal Telecommunications System-2000 (FTS-2000) 150

2. Tactical ISDN 150

3. Security-Related Applications 151

4. ISDN Interoperability with Defense Data Network (DDN) 152

5. Miscellaneous 152

APPENDIX A. ACRONYMS 154

APPENDIX B. JCS SM-684-88 DEFINED C3 ARCHITECTURES 158

APPENDIX C. MAJOR STANDARDS-DEVELOPMENT ORGANIZATIONS . 160

APPENDIX D. OSI REFERENCE MODEL LAYERS 164

LIST OF REFERENCES 168

BIBLIOGRAPHIES 173

INITIAL DISTRIBUTION LIST 175

LIST OF TABLES

Table II-1: Pilot Internet Multiplexers 13

Table III-1: DoD Military Standard Protocol Documentation 49

Table IV-1: ISDN Bearer Services 75

Table IV-2: ISDN Channel Functions/Applications 84

Table IV-3: Comparison of X.25 and CCITT SS7 97

Table V-1: Narrowband and Proposed Broadband Channels 106

Table V-2: Comparison of Packet, Frame and Cell Relay 115

Table V-3: SONET Rates 118

Table VI-1: NIU-Forum Conformance Test Specifications Status 139

LIST OF FIGURES

Figure 1: Near-Term Tiered Implementation 15

Figure 2: Concept of DISN Far-Term Architecture 18

Figure 3 ITA Target 21

Figure 4: Target Base Infrastructure 23

Figure 5: DISN Common User Evolution 24

Figure 6: Functional Architecture of the Copernicus Building Blocks 26

Figure 7 Copernicus Building Blocks 27

Figure 8: The Pillars of the Copernicus Architecture 29

Figure 9: Projected Architecture: Systematic and Network View 36

Figure 10: OSI Reference Model Layers 40

Figure 11: GOSIP Version 2 OSI Architecture 41

Figure 12: DoD Protocol Model 46

Figure 13: DoD and Other Protocol Comparisons 50

Figure 14: Framework for OSI Security 63

Figure 15: Basic ISDN Architectural Model 68

Figure 16: Conceptual View of ISDN 70

Figure 17: Layered Protocol Structure 73

Figure 18: Basic Rate Interface (BRI) 78

Figure 19: Primary Rate Interface (PRI) 80

Figure 20: LAP-D Frame Format 86

Figure 21: TEI and SAPI Address Field Format 87
Figure 22: SS7 Protocol Architecture 91
Figure 23: Conceptual View of SS7 Network 96
Figure 24: B-ISDN Protocol Model for ATM 107
Figure 25: B-ISDN Architecture 110
Figure 26: SONET STS-1 Format 117
Figure 27: Conformance Testing 132
Figure 28: Protocol Implementation Conformance Statement (PICS) 134
Figure 29: Protocol Conformance Test Report (PCTR) 135
Figure 30: System Conformance Test Report (SCTR) 136
Figure 31: Interoperation Testing 143

ACKNOWLEDGEMENT

My deepest thanks go to my advisors, Professors Y.S. Fu and Myung Suh, in the development of this thesis. Professor Fu was the nucleus in providing materials to ensure the accuracy of information regarding the DISN and implementation strategy. He always gave freely of his time to resolve conflicts and kept my motivation level high. I am indeed grateful for his continued support and understanding.

If there was ever a person with interminable technical expertise and patience, it is Professor Suh. Technologies within the computer and communications disciplines evolve at a phenomenal rate and are extremely complex. Obtaining the most current technical information in the area of open systems is almost insurmountable. Professor Suh's persistence aided immensely in helping me analyze the impacts of these new technologies on the DISN. He was always available to answer the multitude of questions and made complex issues more understandable.

Acknowledgement is also extended to Professor Michael G. Sovereign. He was the catalyst in narrowing my area of research and eliminating ambiguities associated with such a broad area. Without his early nurturing of my thesis, I'd still be floundering. For this I am extremely appreciative.

Last but most important I want to thank my beautiful and lovely wife, Vera, for seeing me through this struggle. She has been the pillar, my inspiration and very best friend. I cherish her wisdom and love. Her support has made an extremely difficult task much easier.

I. INTRODUCTION

A. BACKGROUND

Significant changes are occurring in the international and domestic environment that impact future Command, Control and Communications (C^3) requirements. Political and economic pressures will result in reduced resource allocations for military forces. This will have a direct impact on the U.S. force structure and the ability of these forces to respond to future contingencies. The rapid pace of advancing technology is also leading to a revision in the nature of modern warfare. One of these factors is new information transmission processing and support capabilities [Ref. 1:p. iii]. These support capabilities must be responsive to aiding the C^3 mission. The unpredictable nature and location of future crises and conflicts demand prompt and precise employment of forces with little preparation time. U.S. forces will have to operate in areas where there is virtually no pre-positioned C^3 infrastructure and where other forms of local support are minimal. A global (as well as deployable) C^3 system capability must exist to meet demands such as wide-area surveillance, intelligence, battle management, and endurance. This requires an increased emphasis on flexibility in C^3 supporting systems in order to respond to regional crises. In addition to being flexible, C^3 system elements must include modular building blocks suitable for augmenting mobile or static war headquarters as contingencies may require [Ref 1:p. vi]. It should provide completely interoperable interfaces with the automatic data processing (ADP), communications,

personnel, and procedures for both the global infrastructure and the tactical elements [Ref. 1:p. vi]. To support C^3 projections throughout the area of operations, a global infrastructure demands the following capabilities [Ref. 1:p. v]: (1) backbone communications, (2) communication gateways to the forces, (3) augmentation for command centers and other nontactical facilities, (4) data processing, applications, and data bases that can be remotely accessed, (5) managing and processing of wide-area sensor systems, including national system support, and (6) intelligence analysis centers and other direct intelligence support. The communications backbone for supporting C^3 systems is an important factor in building this global interoperable infrastructure. This communications backbone is called the Defense Communications System (DCS) which is operated by the Defense Information System Agency (DISA). The DISA has proposed a high-speed fast packet digital network for the DCS which is called the Defense Information System Network (DISN), for DoD-wide use. It will have Broadband Integrated Services Digital Network (B-ISDN) capabilities based on Asynchronous Transmission Mode (ATM) and Synchronous Optical Network (SONET) and will interface with such technologies as Fiber Distributed Digital Interface (FDDI) and frame relay. The DISN will employ commercial-off-the-shelf (COTS) products conforming to Open Systems Interconnection (OSI) standards[1]. OSI is a new architectural framework designed to achieve data communications standardization on an international basis. These

[1]GOSIP Version 2 does not include these technologies but will be introduced in later versions as the standards are approved by CCITT.

standards are based on a concept called "open systems." The following quote from Baldo and Levan [Ref. 2:p. 3] provides one of many definitions of open systems:

> A set of one or more computers, the associated software, peripherals, terminals, human operators, physical process, means, etc., that forms an autonomous whole capable of performing information processing and/or information transfer.

Government Open System Interconnection Profile (GOSIP) is a subset of the OSI and defines the federal standards for data communications services. It is a mandated standard which must be used by all agencies in the procurement of new data communications equipment or enhancements to existing systems. The framework for future military network architectures shall be based on this new GOSIP standard.

B. PROBLEM

The rapidly changing world environment from the post-Cold War era has instinctively caused a shift in the evolving national military strategy. One of these changes is the consolidation of existing theater C^3 facilities and equipment within a global infrastructure. To keep pace with these global changes means changes to the supporting infrastructure to meet the ever increasing requirements for integrated communications. However, like the rapidly changing world, technology is also rapidly changing.

Most of the C^3 support systems among today's Military Departments (MILDEPs) are standalone and represent a large installed base of multiple vendor communications systems, computer mainframes, minicomputers, and terminals. These systems lack certain features such as increased functionality, modularity, interoperability, flexibility,

and survivability. The MILDEPs (or Services) have developed individual network architectures to provide information to and from both deployed forces and national decisionmakers. These architectures are unique and consist of a number of incompatible proprietary subsystems which are not interoperable.

To build flexibility and modularity required by the changes in todays climate requires interoperability between these disparate architectures to support worldwide contingency requirements. In addition to these unique networks, the MILDEPs have begun to investigate the feasibility of ISDN and deploy this technology to support intra- and inter-base requirements. GOSIP Version 2 has incorporated the use of ISDN as a digital subnetwork technology for high-speed simultaneous voice, data, and image transmission. However, ISDN products by different vendors may have embedded functions that are incompatible with other vendor implementations at various layers. COTS ISDN products must be certified GOSIP-compliant as required by the Federal Information Processing Standards (FIPS)[2]. The North American ISDN Users' Forum (NIU-Forum), under the auspices of the National Institute of Standards and Technology (NIST), develops test suites for ISDN.

The proposed common-user DISN will be based on employing leading edge COTS technologies and must be certified GOSIP-compliant. Although the C^3 community will use COTS products to satisfy their processing needs, integration of these subsystems encompassing these new technologies becomes a real challenge. COTS products must

---

[2]It should be noted that conformance testing does not guarantee that these GOSIP-compliant products will interoperate.

meet requirements beyond that of a benign environment. Additional requirements of increased functionality, interoperability, modularity, flexibility, and survivability must be taken into consideration. The testing and certification of these products should provide a high degree of in meeting all these requirements.

This thesis focuses on meeting interoperability requirements through conformance testing based on the lower layers of GOSIP standards. An overview of fixed Army, Navy, and Air Force network architectures for supporting the C^3 environment and the evolution of the DISN will be presented.

C. GUIDE TO THE FOLLOWING CHAPTERS

1. Chapter II

This chapter describes the DISN in detail and the phased approach for reaching the goal of full integration on a global scale. An overview of the MILDEPs network architectures is also introduced. Collectively, these architectures provide the decision maker with a fused picture of information needed to support the mission.

2. Chapter III

The need for open system standard protocols and the evolution of OSI are described. A detailed discussion of GOSIP is provided along with the migration from the existing Department of Defense (DoD) Transmission Control Protocol/Internet Protocol (TCP/IP). Future versions of GOSIP are also addressed.

3. Chapter IV

This chapter provides details about ISDN and Signalling System 7 (SS7) in particular. This chapter describes ISDN within the framework of the OSI Reference Model and concentrates on its lower three layers.

4. Chapter V

This chapter introduces B-ISDN and discusses evolving technologies such as FDDI, frame relay, SONET, ATM (cell-relay), and Switched Multi-megabit Data Service (SMDS).

5. Chapter VI

Conformance testing is paramount in ensuring interoperability. This chapter discusses conformance testing and describes the conformance testing processes. To be examined are test laboratories at the national, private, DoD and Service levels. It concludes with a discussion of available ISDN Conformance Test suites available for perform conformance testing.

6. Chapter VII

This chapter provides a summary of the need to test to standards in the evolution of the DISN. Potential thesis topics are also discussed for readers interested in ISDN, B-ISDN, GOSIP and open systems interoperability in general.

II. C^3 SYSTEMS ARCHITECTURE

A. BACKGROUND

In DoD terminology, a C^3 system generally refers to a combination of hardware, software, methodologies, and users that perform an information-management function [Ref. 3:p. 11]. The architecture for a C^3 system is defined as "the arrangement of...the basic elements of a C^3 system into an orderly framework." This definition could apply to a relatively small C^3 system, such as a fire control system, as well as to the largest system, the National Military Command System (NMCS). [Ref. 4:p. 67] Primarily the NMCS architecture addresses partitioning and interfaces. Interfaces include external interfaces between the system and its outside world and internal interfaces join parts of the system which are acquired independently. JCS SM-684-88 defines five separate types of architectures [Ref. 5:p. 3]: (1) System Architecture, (2) Mission Area Architecture, (3) Subordinate or Component Architecture, (4) Theater Architecture, and (5) NMCS Architecture. One other type of C^3 architecture which was not addressed in JCS SM-684-88, is the Service Architecture. Each of these architectures are discussed in Appendix B. This thesis focuses on two of these architectures--Mission Area and the Service Architectures.

Given the size of the military, an inventory of C^3 computer and communications systems reveals an incredible investment in supporting these architectures. During the past decade, military organizations were free to purchase equipment deemed necessary

to meet mission requirements. Much of this equipment was procured without structure or guidance in building a cohesive interoperable infrastructure. As a consequence, interoperability was nonexistent. There was no real requirement at the time for such interoperability. Today it has become increasingly important to exchange information beyond that of parochial organizations. To promote migration to a full interoperable environment, an integrated information transfer infrastructure, called the Defense Information Systems Network (DISN) has been proposed. This integrated network will be built in conformance with the open network standards as specified in GOSIP.

B. EVOLUTION OF THE DEFENSE INFORMATION SYSTEMS NETWORK (DISN)

1. Background

DISA is responsible for providing architectural development for national, joint, and combined C^3 systems (such as the NMCS, WWMCCS, DCS, and MILSATCOM) that support the NCA, CJCS, and CINCs. Their primary mission, in terms of open system, is to enforce standards testing based on GOSIP standards. DISA also provides direct technical support to the CINCs in the development of C^3 assessments and architectures [Ref. 5:p. 1]. MILDEPs environments consist of circuit switching (for voice) and dedicated lines for low-volume traffic. Growing needs, however, have forced a reexamination of these C^3 environments. One of the concerns indicated that there is a rapidly developing need for integrated voice, data and video. This could so far have been supported by dedicated lines such as T-1 which runs at 1.544 Mpbs, the need is

rapidly surpassing this capacity. Providing support for the C^3 systems is not easy given the complexity of todays technologies and the various Services (or MILDEPs) and Agencies (S/A) networks. Technology and requirements have shifted to the need for high-speed fast packet switching. DISA's proposal for an integrated network is one step to make interoperability a truism between inter- and intra-theater environments. This high-speed fast packet-switching integrated digital network is based on B-ISDN [Ref. 6:p. 2]. This new network is called the DISN and aimed at providing full integration for the C^3 communities.

2. Existing DoD Network Architecture

The DCS is a worldwide complex of DoD communications networks. It includes all worldwide, long haul, government-owned and leased, point-to-point circuits, trunks, terminals and control facilities; it consists of microwave, troposcatter, landlines, submarine cables and voice frequency telegraph circuits. The DCS is essentially viewed as a collection of independent common-user subsystems, each designed to provide a unique service and travels on the common-user backbone transmission system. Major subsystems of the DCS include [Ref. 7:p. 4-24]:

- Defense Commercial Telecommunications Network (DCTN): DCTN is a leased communications operated by DISA. It is designed to provide the services a routine common-user switched voice, dedicated voice/data, and video teleconferencing services throughout the United States. It is a fully integrated digital system that uses a mix of satellites and terrestrial transmission paths. It has approximately 272 service delivery points within the CONUS. The DCTN contract terminates in March 1996.

- Defense Data Network (DDN): The DDN is a worldwide digital packet switched long-haul network. Operated by DISA, the DDN consists of four separate networks operating at different security levels: Military Network (MILNET

[unclassified]), DSNET 1 (secret), DSNET 2 (top secret) and DSNET 3 (SCI). The DDN is detailed further in Chapter III.

- Defense Switched Network (DSN): The DSN is the primary DoD telecommunications network evolving from AUTOVON. It will provide multi-level precedence and pre-emption (MLPP) services in conjunction with the Red Switch and Secure Telephone Unit III (STU-III) projects of the Secure Voice System. Upon full implementation in the mid-1990s, the DSN will interconnect all U.S. military bases worldwide to provide terminal-to-terminal, long distance common user and dedicated telephone, data, teleconferencing, and video services.

Voice and low-speed data have always been the dominant service provided by the DCS. However, due to the increased demand for high-speed data communications and multimedia services, the advent of new multiplexing/networking technology, and the need for cost competitiveness, the DCS must evolve from the current environment to a fully integrated digital DISN. Complicating this problem is the incorporation of other Services' and Agencies'(S/A) network initiatives. The S/As are individually pursuing integrated networks to be built from COTS products. Examples include the Air Force Integrated Telecommunications Network (AFNET) Program and the Navy Network (NAVNET) Program and the Defense Logistics Agency's (DLA) DLANET. The DISN plans to employ a shared communications backbone operating at SONET transmission rates to meet the growing needs in voice, data, video, and imagery communications requirements.

3. Technology Considerations

Wide area networks (WANs) permit users from one part of the country to communicate with another transparently. The Department of Defense (DoD) has built

a number of networks that comprise the DCS for this purpose. However, the explosive growth in user needs have out grown the capabilities, in terms of bandwidth and services, of the DCS. Merging and evolving technologies, coupled with increasing demands for efficient and timely collection, processing, and dissemination of information, are leading to development of integrated systems that transmit and process all types of data.

ISDN was devised to provide a global, efficient, flexible, and cost effective end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard multi-purpose user-network interfaces. Its aim is to integrate existing services and new technologies into a single network. ISDN can also be used effectively to interconnect local area networks (LANs). Frame relay is a service offered over ISDN to interconnect geographically dispersed LANs. It offers the advantage of increased throughput because the overhead of error detection and recovery is eliminated. However, the user needs will be rapidly outgrowing the bandwidth of ISDN and frame relay services too. Advances in computer and signal-processing technology have led to the emergence of multimedia applications combining voice, data, video and graphics. ISDN will not be sufficient to meet this increasing need for very high-speed video services. The expected increase in user requirements has spawned the development of high-speed packet-switching technology such as B-ISDN which is based on ATM cell-relay. It is designed to support extremely high data rates. Once in place, it could eliminate the need for SMDS and frame relay. However, Switched Multi-megabit Data Service (SMDS) and frame relay, "islands" in metropolitan areas like ISDN, are expected to interface to a B-ISDN

backbone. To migrate the current network architecture from its current state to B-ISDN will require careful planning. This plan requires a continuous evaluation and testing of new technologies. The next section describes the various phases of this migration and DISA's approach for moving to the DISN backbone.

4. DISN Phased Development

DISA has proposed a phased approach to provide intra- and inter-theater interoperability. The phases include the near-term, transition phase[3] and far-term. The near-term (Phase I) is primarily aimed at reducing cost by implementing a concept called circuit bundling. The mid-term (Phase II) is designed to evolve ISDN and finally, the far-term (Phase III) involves the implementation of B-ISDN. The far-term will be based on leased services. Each of the phases are discussed in some detail below.

a. Near-Term Description and Approach

Phase I near-term is designed to cover from the present period to three years out. It is aimed at satisfying three immediate requirements [Ref. 6: p. 7]: (1) reducing cost by circuit bundling, (2) expansion of the Pilot Internet, and (3) S/A network consolidation. The ultimate design goal of circuit bundling is to reduce cost by decreasing the number of individual circuits supporting the various Services. DISA believes this can be done without compromising operational requirements, quality of service, and survivability in support of the C^3 environment. Many of the MILDEPs are

---

[3]Officially, DISA does not recognize a mid-term phase within the evolution of the DISN. However, there is an interim phase that must occur between the near- and far-term. The thesis will refer to this as a transition phase.

using switched data and point-to-point (e.g., dedicated) circuits to support C^3 long-haul requirements. These lines are generally 56 kbps to 1.544 Mbps leased circuits and for supporting high volume traffic. DISA recognizes that the lease cost of four to six DS-0 (64 kbps) circuits is generally equivalent to the lease cost of a T-1 (1.544 Mbps) line, and the cost of eight to ten T-1 lines is generally equivalent to the lease cost of a T-3 (44.736 Mbps) circuit. Therefore, the use of smart multiplexers (digital crossconnect systems) can offer substantial savings. Smart multiplexers dynamically allocate DS-0 (64 kbps) channels to different applications [Ref 8:p. 1]. The second initiative under the near-term is the Pilot Internet. The Pilot Internet is designed to be the pre-DISN but it does not employ ISDN or evolving B-ISDN technology. It consists of BBN T-500 multiplexers installed at Ft Lewis[4], Stanford Research Institute (SRI), ISI, Ft Huachuca, Randolph AFB, Gunter AFB, Ft Benjamin Harrison, Ft Detrick, Ft Belvior, and Center for Engineering (CFE) [Ref. 6:p. 8]. However, due to funding problems among the participants, it really never gained prominence or momentum [Ref 9]. It is still, however, operational. The third initiative is the consolidation of the S/A private networks. S/A consolidation is designed to provide internet gateways between the S/A-unique networks (e.g., AFNET, NAVNET, DLANET, and eventually the Pilot Internet). The multiplexers currently being used by these organizations are listed in the table on the following page.

[4]The internet site at Ft Lewis consist of a C/300 and a CISCO IP router instead of a T-500.

TABLE II-1
PILOT INTERNET MULTIPLEXERS

Service/Agency	Type Multiplexer	ISDN Capable?
Air Force	IDNX[5]	No
Navy	Timeplex	Yes
Defense Logistics Agency	Paradyne	Yes
Pilot Internet	T-500	No

For at least two years, DISN will use multiplexers provided by AT&T, Simplex and Network Equipment Technology (N.E.T.) Federal Incorporation to help satisfy this initiative. However, the AFNET contract which uses N.E.T. equipment was declared as the DoD standard [Ref. 10:p. 37]. The Phase I envisions the implementation of a tiered network structure. These three tiers are [Ref. 6:p. 4]: (1) a smart multiplexer layer (tier 3), providing T-1/T-3 switching capability to provide circuit bundling and full T-1 service to the customers, (2) the subnetwork layer including X.25 packet switching services (tier 2), and (3) an IP layer (tier 1) for connecting intra-base LANS using T-1. Figure 1 provides an illustration of this tiered implementation [Ref. 6:p. 4].

b. Transition Phase Description and Approach

Phase II is an outgrowth of the near-term. This phase is expected to be implemented between the 1994-1996 time-frame [Ref 9]. There are basically two

[5]Integrated Digital Network Exchange (IDNX) uses unchannelized bit streams at rates of 1.544 Mbps. Actual usable bandwidth is 1.516 Mbps--28 kilobits are used for overhead and network management.

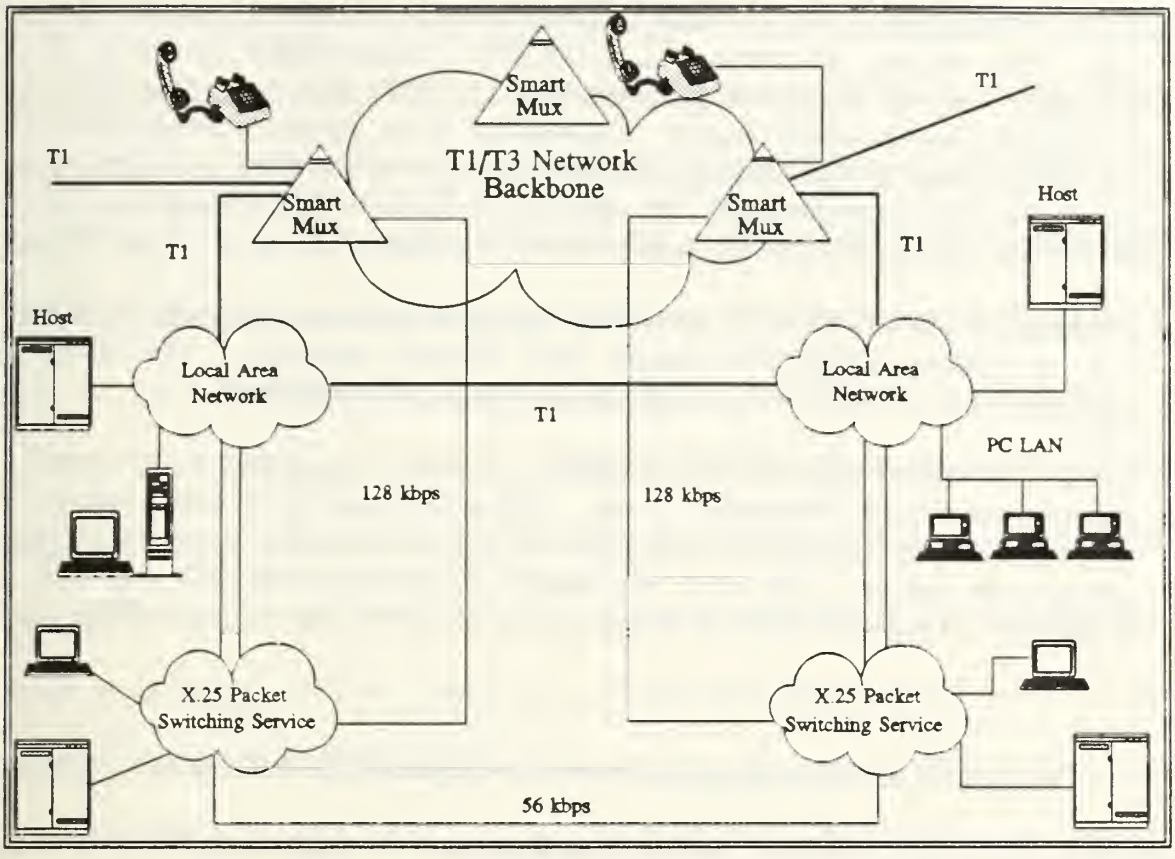


Figure 1
Near-Term Tiered Implementation

initiatives involved with this phase, both aimed at providing ISDN services. The first initiative is designed to offer the users the following capabilities [Ref. 6:p. 5]:

- Switched voice service by providing digital transmission to transport Defense Switched Network (DSN) voice and data (via modems) on interswitch trunks or trunk groups from the user's facility to the designated DSN tandem voice switching center.

- Circuit switched data service by providing dial-up, full duplex, synchronous, 56 kbps (64 kbps when clear channel capability is available) from the user's facility to the DSN switching network. If the user's facility does not have a digital switching capability, dedicated digital access to the DSN can be provided.

- Packet switched service by providing a packet transport and switching service for data. This service will conform to the CCITT recommendation for the X.25 protocol, currently offered as DDN Basic X.25, while also supporting DDN Standard X.25 to the extent possible. The majority of this packet switched service will be provided by the existing MILNET segment of the DDN. To ensure government-wide interoperability, the transition to GOSIP will be accomplished in accordance with the FIPS 146-X and under ASD guidance.[6]

- Internetwork gateway service by providing high speed gateway services delivering T-1, or greater, information transfer rates between networks. The initial implementation of DISN will provide this service for IP subscribers.

- Voice and audio/graphics teleconferencing service by providing a dedicated transmission channel between two points. This service exists to permit a user to interconnect customer premise equipment (CPE) that are not members of a common-user system. The users will manage bandwidth within their allocated assignment. The bandwidth will be provided at each user location at the POP.

The second part of the transition phase involves installing ISDN switches onto the AFNET, NAVNET, DLANET and the Pilot Internet. The interface to the users in the near-term will eventually include ISDN primary rate interface (PRI). The second initiative leading toward ISDN involves a CONUS-wide ISDN trial network. Although scheduled to officially begin 1 September 1992, it is envisioned as the interim step toward B-ISDN [Ref. 9]. Participants include the Air Force, Army, Navy, and the Marine Corps and could total more than 10 sites. The ISDN trial will include a variety of heterogeneous equipment such as AT&T 5ESS, Northern Telecom DMS-100s, SL-100 and Meridian, and Teleos access equipment. The purpose of the network is to evaluate

---

[6]This guidance is addressed in ASD/C3I Memorandum, Subject: Open Systems Interconnection Protocols, dated July 2, 1987.

its performance using operational processing. Essentially, it is designed to evaluate the cost of leased lines versus ISDN in terms of performance. The trial or demonstration concludes 1 October 1993, however, the staff at DISA insists that this is not really a trial but will evolve as an operational network shifting to the far-term architecture [Ref. 9]. DISA is funding for network services and access lines through the one-year trial period.

c. Far-Term Description and Approach

This phase implements B-ISDN. The aim of this phase is to allow a migration to open systems networks which have fewer DoD-unique features and vendor proprietary designs. This will also permit extensive use of COTS. As stated earlier, much of the far-term DISN is dependent on such technologies as cell relay (ATM), SONET, and FDDI. Technologies in these areas are growing at a phenomenal rate. Industry vendors are aggressively producing cell relay to also include SMDS. DISA's strategy for implementing the far-term is through "full integration." The full integration approach used here is based on satisfying total traffic requirements, facility locations, and performance specifications to determine the most cost-effective DISN topology, size, and hardware and software specifications. Figure 2 shows a conceptual view of the end goal DISN [Ref. 6:p. 11]. This approach standardizes equipment and optimizes network topology, backbone size and access circuits. Cost, risk, and network size are the basic factors driving the right approach. DISA plans to upgrade the digital switches, such as the AT&T 5ESS and 4ESS and the Northern Telecom's DMS-100 and DMS-250 used in the DCS, to B-ISDN. The end goal of DISN is to support a wide variety of network services with access rates up to 150 Mbps. However, B-ISDN technology can operate

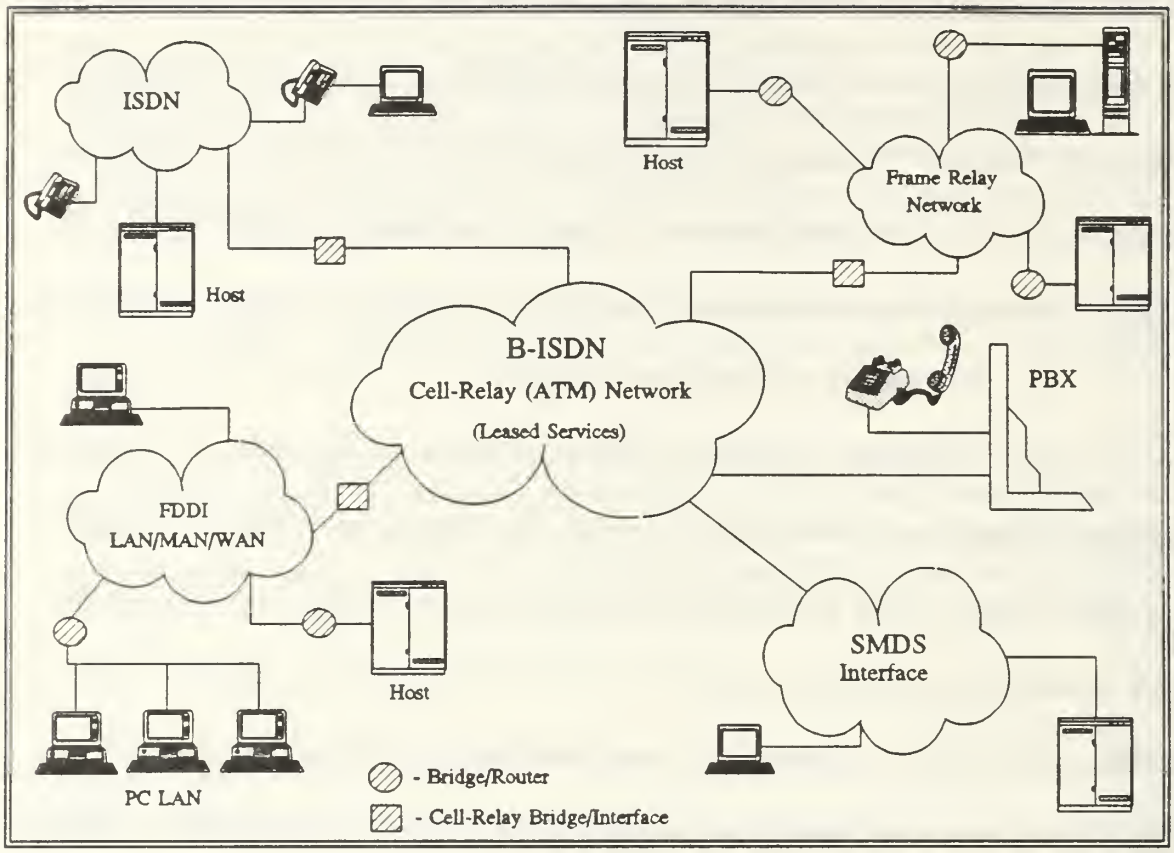


Figure 2
Concept of DISN Far-Term Architecture

at speeds four times this rate and will no doubt be used to support the C^3 subsystems. The Request for Proposal (RFP) for the DISN Far-Term will be released in 1995 and the contract is expected to be awarded prior to expiration of the DCTN contract [Ref 10:p. 37]. It is anticipated that the B-ISDN effort will begin around the year 2000.

C. MILITARY DEPARTMENT ARCHITECTURES

The development of Service-unique architectures has been going on for years. Many of these architectures were developed out of mission necessity and without a well-defined framework. They suffered from the lack of guidance, control, and immature standards. To facilitate intra-service interoperability, many services elected a "black box" approach consisting of bridges, routers, and/or gateways. Rather than purchasing new state-of-the-art equipment or retrofitting current systems with open systems standards, these specially developed devices have become an integral part of the infrastructure to interconnect heterogeneous computers and disparate networks. Collectively, this architectural framework is designed to provide the end user (the decision maker) with a timely fused picture of information needed to support the mission. Strategic efforts are underway to incorporate open systems and COTS into the MILDEPS operational networks. What follows is a discussion of the various MILDEP network structures, deficiencies, and their strategies for evolving to the open systems network architecture defined by the DISN.

1. Air Force Information Transfer Architecture (ITA)

a. Purpose and Objectives

The Air Force's technical architecture include several building blocks: information transfer, integrated systems control, deployable, security, software, data management, and automated systems support [Ref. 11:p. 1]. These building blocks support the overall Air Force Communications and Computer Systems Architecture (AFCSA). Information transfer, which encompasses both intra- and inter-base

communications, is a key element in the AFCSA. The Information Transfer Architecture (ITA), addresses current capabilities, describes target capabilities, and provides for the evolution and transition strategies to the target. A schematic of this target architecture is shown in Figure 3 [Ref. 11:p. 1]. The ITA has three purposes:

1. It is the basis for a single, common, integrated digital base-level communications-computer systems infrastructure of voice, data, video, and telemetry connectivity requirements, including access to inter-base systems.

2. It provides guidance for developing long-haul information transfer systems and networks that support Air Force command and control and mission support needs.

3. It defines how to satisfy evolving throughput, interoperability, flexibility, security, survivability, and availability needs.

One of the technical objectives of the ITA is to provide a seamless fixed/deployable communications-computer system using standard hardware components, open systems software and architectures. This seamless connectivity is provided through a number of ITA transport systems and networks which include as the Defense Satellite Communications System (DSCS), DDN, DSN, and specifically the AFNET.

AFNET is a Service-unique CONUS high capacity inter-base information transport utility for supporting voice, data, and video. It is best described as an intelligent or a virtual private network (VPN). A VPN refers to a family of software defined services like uniform numbering plan, customer-specified routing, originating screening, bandwidth on demand, or other user-specified voice and data services. The AFNET currently employs digital switches and smart multiplexers to provide many of these services. The design objective for this intelligent autonomous network is to bundle user requirements and provide these types of services for less money [Ref. 11:p. 7].

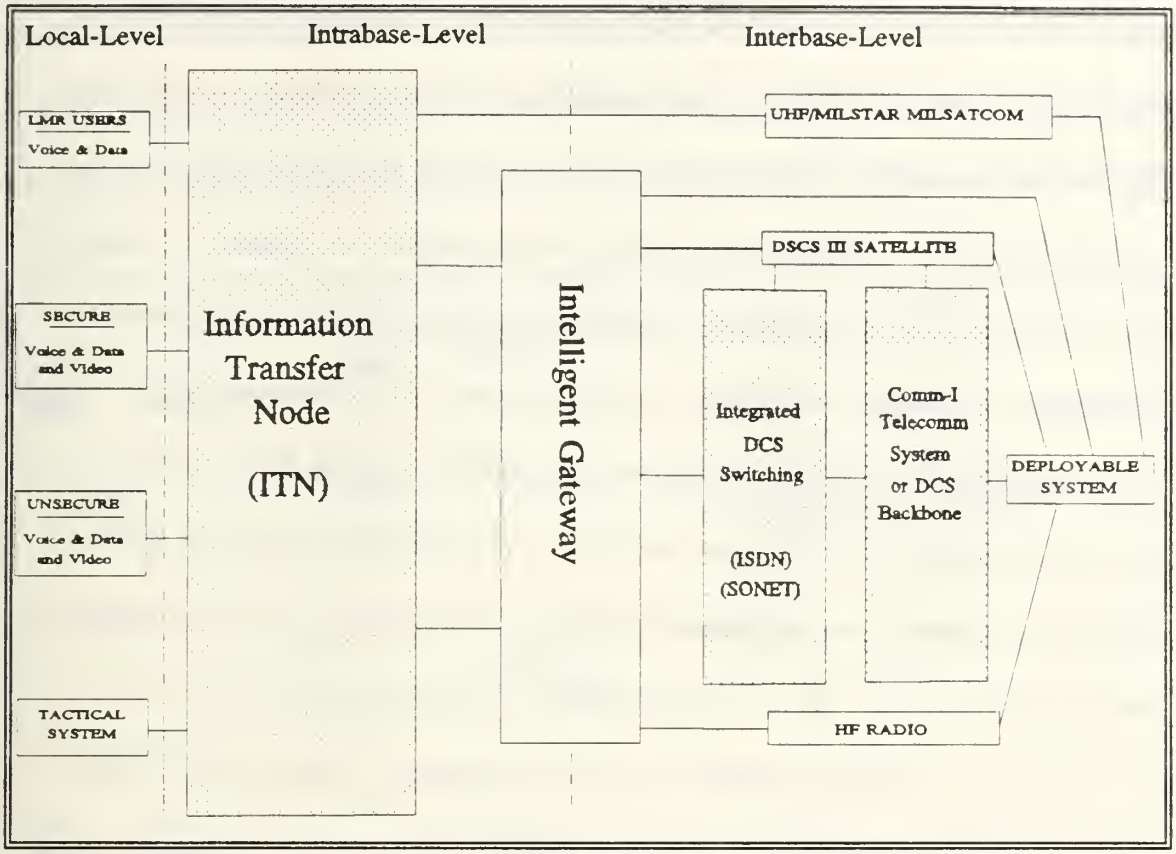


Figure 3
ITA Target

ISDN switches such as those used on the DCS are also being deployed by the Air Force, but not necessarily under the AFNET initiative.

b. Deficiencies

The Air Force notes three areas of deficiencies that generally exist in data networks: (1) local level, (2) intra-base level, and (3) inter-base level. Within the Air Force, these deficiencies mostly consist in incompatible proprietary networks which support a variety of functional and departmental needs with varied topologies. In terms of inter-base (joint level) support, the existing Tri-Service Tactical (TRI-TAC) equipment

is antiquated. It uses circuit switching protocols and topology used in the current tactical communications. However, while extremely capable in the digital tactical network, they have limited interoperability with fixed switching networks and local users due to differences in protocols, multiplexing schemes, and signalling techniques. Unique protocols and interface specifications have resulted in tactical systems that are inflexible. The proliferation of user-provided computer driven systems, when deployed, forces the tactical communications and computer systems to attempt to prepare for a plethora of requirements that are, for the most part unknown. The Air Force maintains that by requiring common standards and equipment with the fixed infrastructure this problem will be overcome. [Ref. 11:p. 9] These issues have been on the forefront of the Air Force's efforts to move to a single integrated digital environment. However, with the innovations of new technologies, the Air Force insist that it must sustain a flexible posture; a position that will track commercial standards and technologies, without fully committing until adopted by the industry as a whole [Ref. 11:p. 20].

c. Target Architecture and Evolution

The Air Force's target architecture was shown previously in Figure 3. The architecture is designed to support both fixed and deployable systems. The Air Force's plans for integrated services is to procure and install hardware and software upgrades which implements ISDN features. This includes upgrading current switching technology and distribution systems to provide basic and primary rates and signalling through Signalling System 7 (SS7). A more detailed view of the Air Force's target architecture is shown in Figure 4 [Ref. 11:p. 13]. The Air Force envisions that both

seamless fixed and deployed systems interoperability will employ the same technology and potentially the same equipment used in fixed locations. Their integrated approach will evolve with the goals of the DISN. Specifically, the evolution will parallel the

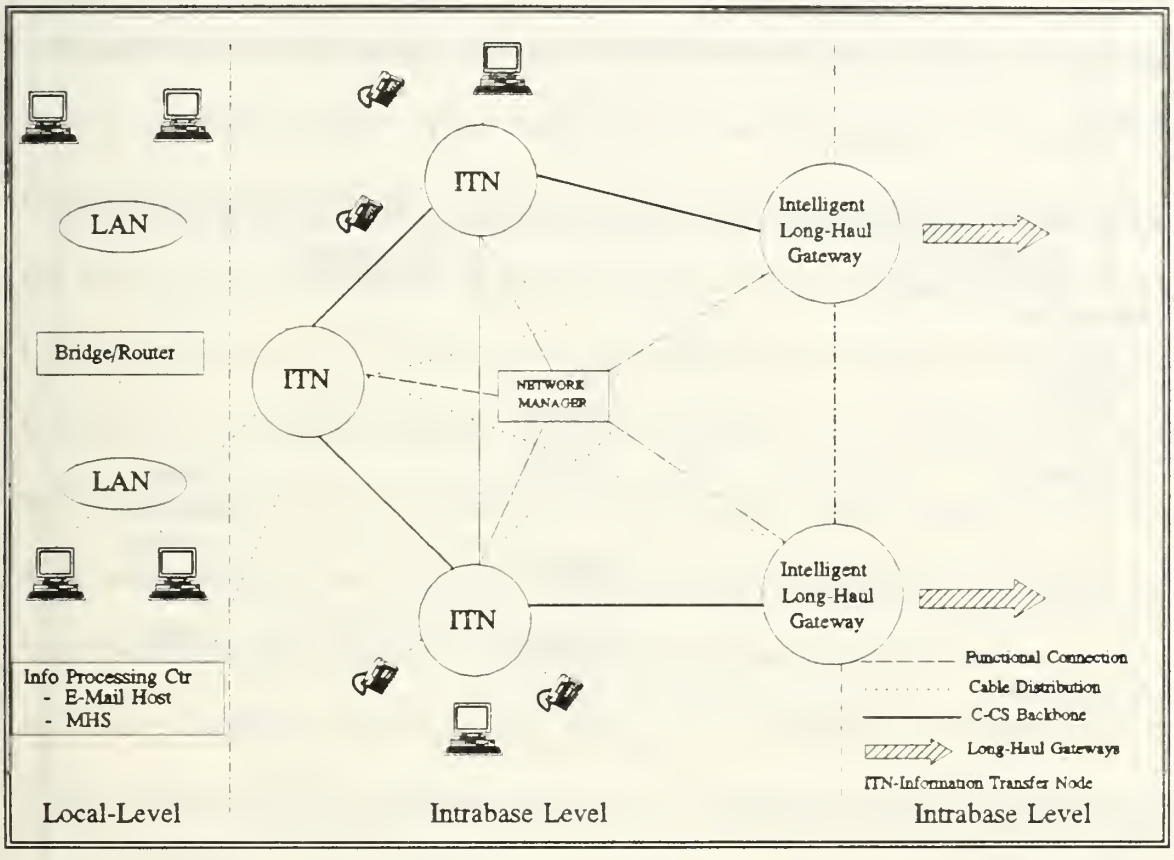


Figure 4
Target Base Infrastructure

common-user and C^2 community efforts. A simplified diagram of the DISN common-user/C^2 evolution is shown in Figure 5 [Ref. 11:p. 19]. The common-user DDN (incorporating the Defense Messaging System) and the DSN will grow with the DISN. The C^2 support structure, designed to assure survivability, addresses network

improvements. The Air Force believes that survivability of long-haul systems can be assured with enhancements in satellite bandwidth usage, coding techniques, and link availability in HF communications. Evolution to the target ITA will occur within the larger context of DoD-wide communications network development. Therefore, the path for evolving this architecture must parallel the efforts being taken in the development of the DISN.

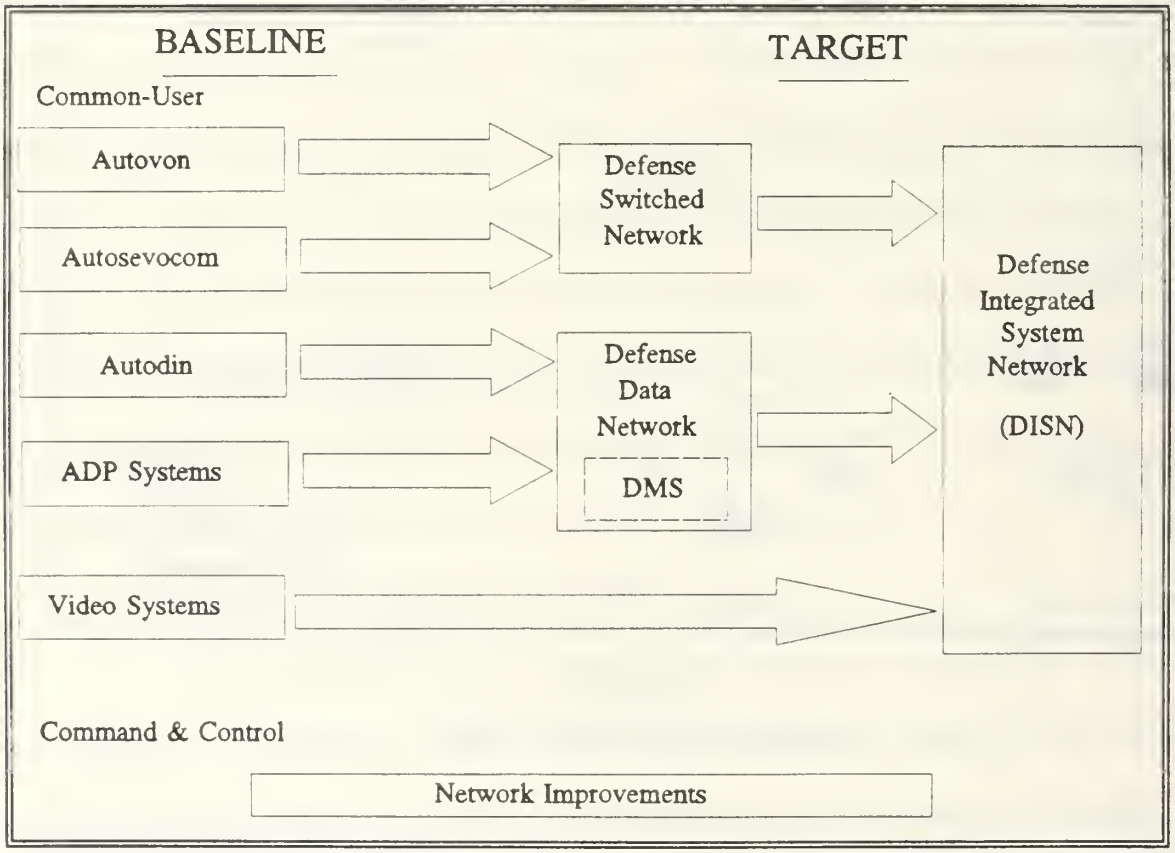


Figure 5
DISN Common User Evolution

2. Navy Copernicus Architecture

a. Purpose and Objectives

Copernicus is the proposed Navy's Command, Control, Communications and Computer (and Intelligence) C4I[7] architecture for integrated land-sea tactical command (e.g., fixed and deployable). Like the Air Force, the Navy's architecture consists of building blocks. These building blocks are called pillars and include: the Global Information Exchange Systems (GLOBIXS), the CINC Command Center (CCC), the Tactical Data Information Exchange (TADIXS), and the Tactical Command Center (TCC) [Ref. 7:p. 3-1]. While all of four are essential to the Copernicus architecture, GLOBIXS are the most important in the development of an integrated shore-based services environment and is highlighted here more than the other three. GLOBIXS is designed to provide an "information exchange" role similar to the Air Force's "information transfer" function. These functions include voice, file transfer, imagery, interactive, messaging, real-time data, and video. GLOBIXS are global networks imposed on the DCS or commercial networks. It combines existing shore sensor nodes, processing centers, and other selected activities into communities of common interest. The technological manifestations of GLOBIXS are derived from four building blocks: (1) network services, (2) hardware, (3) operating systems, and (4) software applications

---

[7]"Intelligence", like computers, is an integral part of the Command, Control, Communications (C^3) infrastructure and should not to be considered a separate entity in regard to C^3 support.

and utilities. Figure 6, is a modified conceptual view of the Copernicus building blocks and how they support the various functional architectures [Ref. 7:p. 4-11].

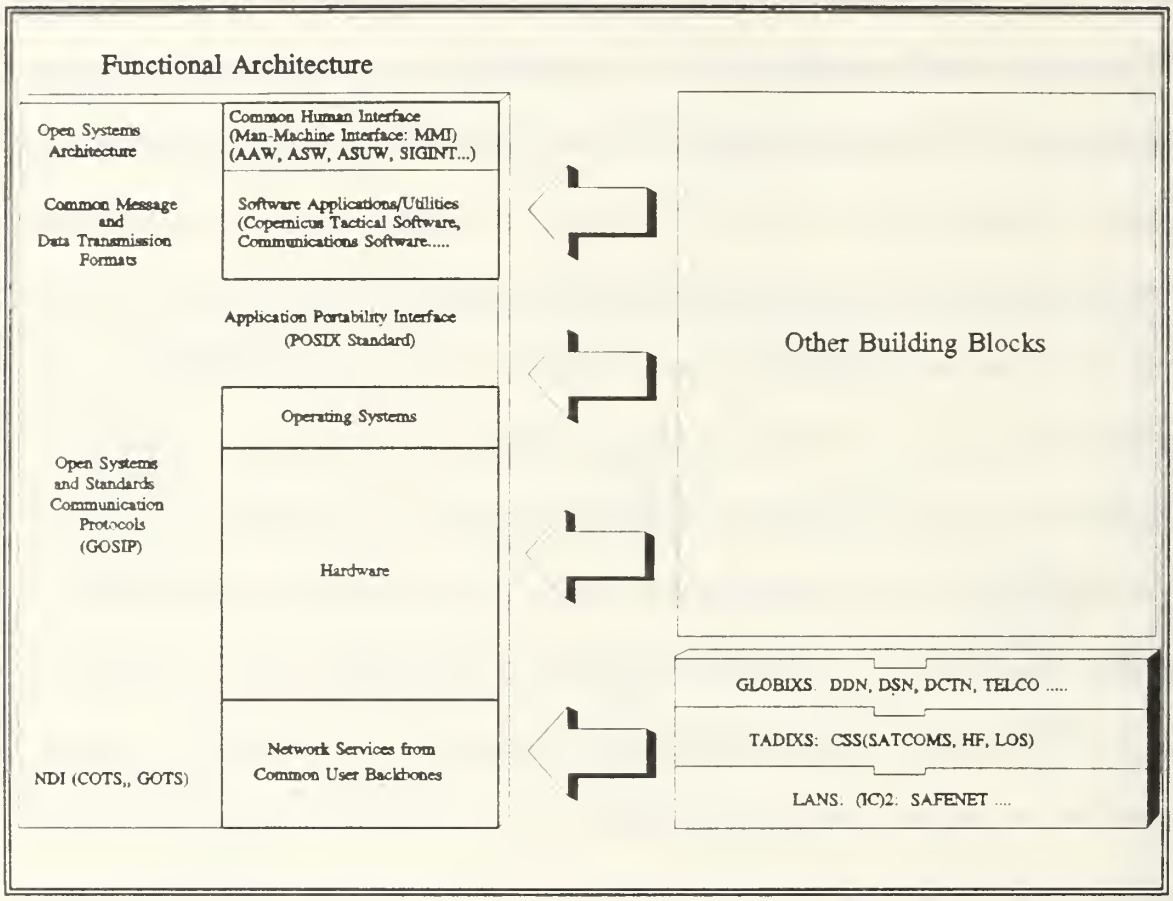

Functional Architecture
Open Systems Architecture
Common Message and Data Transmission Formats
Common Human Interface (Man-Machine Interface: MMI) (AAW, ASW, ASUW, SIGINT...)
Software Applications/Utilities (Copernicus Tactical Software, Communications Software.....
Application Portability Interface (POSIX Standard)
Operating Systems
Open Systems and Standards Communication Protocols (GOSIP)
Hardware
Network Services from Common User Backbones
NDI (COTS,, GOTS)
Other Building Blocks
GLOBIXS: DDN, DSN, DCTN, TELCO .....
TADIXS: CSS(SATCOMS, HF, LOS)
LANS: (IC)2: SAFENET ....

Figure 6
Functional Architecture of the
Copernicus Building Blocks

Only the network services portion of the architecture is shown as it relates to GLOBIXS and TADIXS. The actual building blocks of GLOBIXS and the other three pillars are shown in Figure 7 [Ref. 7:p. 8-3]. Clearly, network services are at the core of both GLOBIXS and TADIXS. The two types of network services within GLOBIXS includes

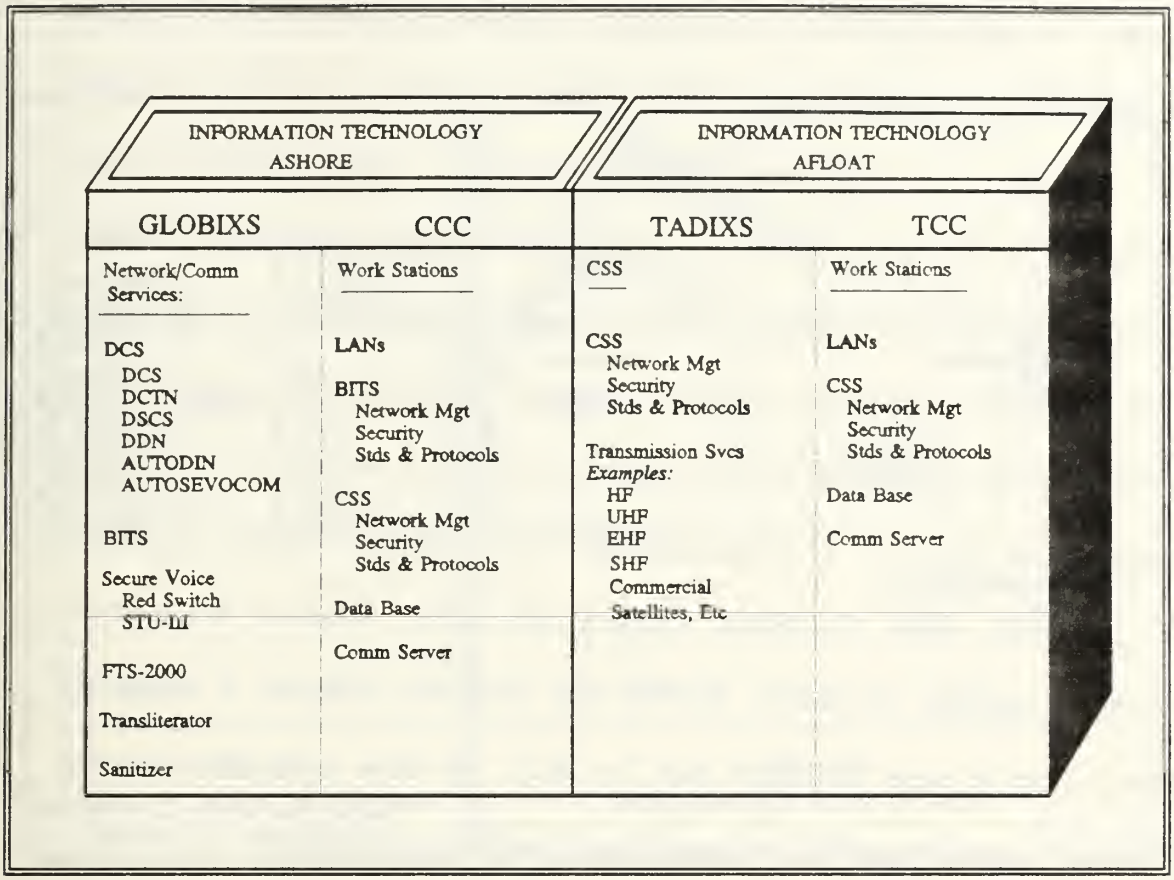


Figure 7
Copernicus Building Blocks

both commercial and government services. These services are available to the common user and based on open systems networks; adapted for the Navy tactical environment. The commercial or government services are generally used to satisfy shore bases or facilities such as headquarters and operation centers, support and administrative centers, and research and development centers. [Ref. 12] The second building block of GLOBIXS is the hardware platform. Most of the hardware building blocks for GLOBIXS exist today; however, selecting a standard building block from the many

duplicative stove-pipe programs will be necessary. Operating systems, the third building block within GLOBIXS, will employ COTS. These will include Unix, VMS, and Ada. The last building block is software applications and utilities. Here, the software will largely be COTS. However, the Navy envisions that all software that is government-unique will be written in Ada [Ref. 7:p. 4-10]. These building blocks are, by definition, joint in construction and some will be combined. GLOBIXS has eight standing components which supports a wide variety of Navy functions and services called "communities of interest." These standing GLOBIXS include: SIGINT GLOBIXS, ASW GLOBIXS, SEW GLOBIXS, Imagery GLOBIXS, Database Management GLOBIXS, Command GLOBIXS, RDIXS, and NAVIXS. Figure 8 shows the interrelationship of these GLOBIXS [Ref 7:p. 8-1]. Of these eight, the Command GLOBIXS is essentially where the migration to an ISDN and B-ISDN will probably occur first. Command GLOBIXS is a multimedia (e.g., video teleconferencing, voice, facsimile, narrative) network, connecting major commands (i.e., numbered fleets, FLTCINCs, component commanders, JTF commanders, USCINCs). A common intersection with GLOBIXS is the CCC. Like GLOBIXS, the CCC is also a virtual network, imposed over metropolitan area networks (MANs) on Oahu, Hawaii, in Norfolk, Virginia, and in Naples, Italy. The CCC will integrate existing command and staff organizations and proposes to construct two new ones--a Space and Electronic Warfare (SEW) Center and a research center. It is expected that the afloat commander will view the CCC as a group of shore-based assistants somewhat analogous to the Composite Warfare Commander (CWC) of the Carrier Battle Group (CVBG) afloat. OSI

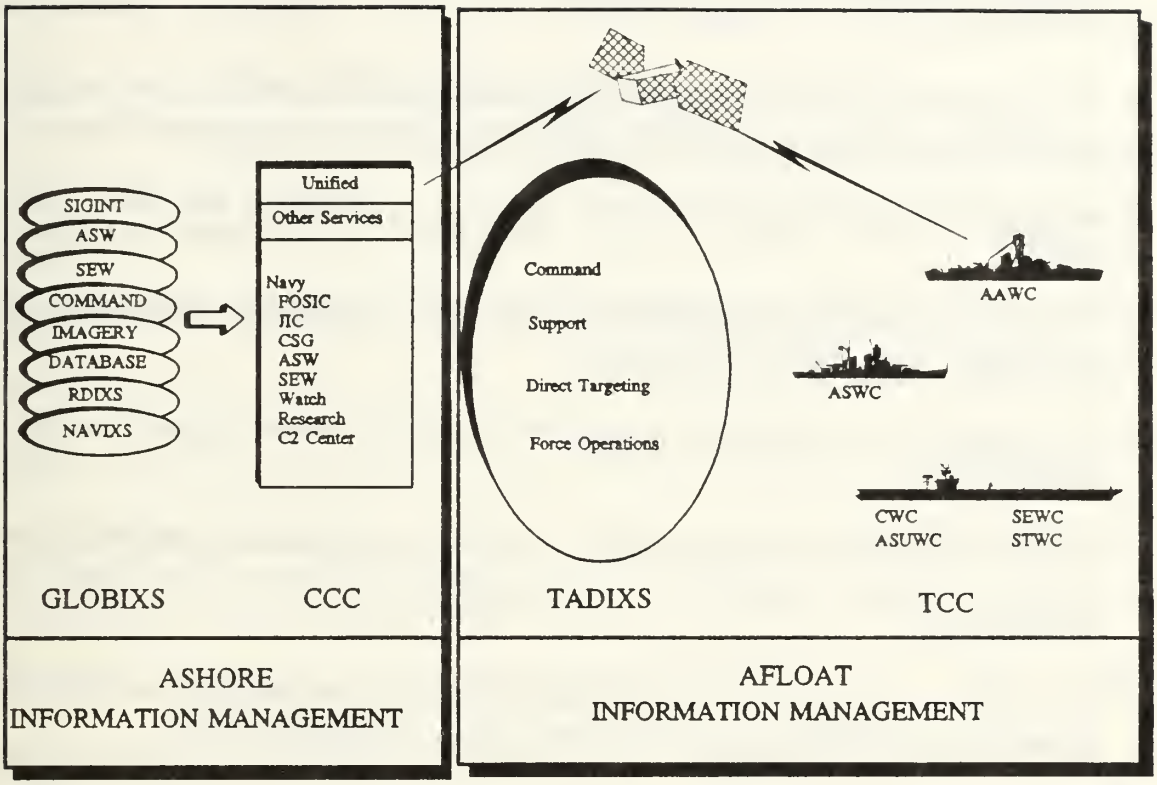


Figure 8
The Pillars of the Copernicus Architecture

designs for TADIXS must be modified in order to meet the afloat requirements. [Ref. 7:p. 3-1]

b. Deficiencies

The Navy identifies eight systematic shortfalls within their current architecture. The shortfalls below are quoted from the Navy's Copernicus Phase I Requirements Definition [Ref. 7:p. 2-1]:

- The first is command and control itself. We are trying to take the threat to our existing C^2 doctrine instead of taking a flexible approach to command and control doctrine based upon the threat;

- We cannot decant operational traffic from administrative traffic; we have no real technological means to gain capacity to support the increased operational tempo;

- Information is conveyed in the wrong format (i.e., messages) and form (i.e., paper);

- The current system supporting narrative traffic and its reflection of diverse sensors and analytic nodes ashore is inefficient;

- The technology of communications and the diversity of communications services is inadequate;

- The incompatibilities of narrative traffic, common displays, computer proliferation, etc have resulted in a significant loss of operational perspective with respect to sensor traffic;

- The result of the Cold War era has brought about the necessity to develop and disseminate information on a far broader category of potential threats;

- Following from the summation of this information, it fosters development of a means to more efficiently disseminate and display intelligence information.

In terms of OSI and GOSIP, the Navy has recognized that there are insufficiencies or differences in applying these standards to GLOBIXS. The OSI Reference Model alone is not sufficient to provide general purpose connectivity. It defines only a framework for a layered architecture; it does not provide the protocol specifications necessary to implement a networking capability [Ref. 7:p. 4-5]. Additionally, while GOSIP may be applicable to GLOBIXS, there are currently

unresolved differences when GOSIP is applied to the tactical RF communications environment supporting voice and real-time tactical information networks.

c. Target Architecture and Evolution

The Navy's Copernicus architecture seeks to forge a single open system for Navy personnel both ashore and at sea. The target involves a single integrated land-sea environment. GLOBIXS is one of the vital pillars in bringing this goal to fruition. GLOBIXS services will be based on commercial ISDN or B-ISDN, federal ISDN/B-ISDN, or GOSIP services [Ref. 12] and, therefore, will make use of both narrowband and broadband technologies. The Navy will use current and planned common-user communications such as the evolving DCS or FTS-2000 to facilitate integration by providing a vehicle for network communications [Ref. 7:p. 4-2]. Other networks available include NAVNET, DDN, and DSNET. Although the DISN is emerging, the Navy anticipates that the DCS will be the primary vehicle to open systems since its network management, administrative, security, and services structure would be most compatible with the GLOBIXS concept [Ref. 7:p. 8-8].

In summary, the Navy's migration to an open systems architecture will be based on the implementation of the Copernicus concept. Through these four pillars, Copernicus will be constructed as an interactive framework that ties together the command and control process of the Navy tactical commander afloat, the Joint Task Force (JTF) commander, the numbered fleet commander and others with the CINCs ashore. Specifically, GLOBIXS (and TADIXS) will involve the use of digital networks

such as DCS and FTS-2000. However, with the emergence of the DISN, the Navy will be able to use this as a transport vehicle between shore bases and the DISN.

3. Army Information System Architecture (ISA)

a. Purpose and Objective

The Army's Information Mission Area (IMA) architecture is dispersed through 13 technical documents called mission areas. These mission families (e.g. information processing, long-haul information transfer, tactical systems interface, etc.), describe the baseline, mid-range architectures and plots a course to the Army's long-range architecture [Ref. 13:p. I-II]. Collectively, these 13 volumes make up the IMA ISA. The Army's fixed information transfer architectures are described in Volumes 3 and 4. They are designed to support information transfer for both intra- and inter-base communications. In support of this requirement, the US Army Information System Engineering Command (USAISEC) proposed that [Ref. 14:p. xviii]:

- Intra-installation communications will primarily be provided by an installation-wide fiber optic backbone network using FDDI;
- An ISDN switching system will support the voice requirements of an installation and the data requirements in conjunction with the FDDI service, and;
- Office/departmental level communications will exist as LANs with gateway capability to installation level services, or as metallic/optical connections to the installation ISDN switch.

The Army identifies four types of switches that may exist at a typical site based on the type used and their ability to transition to ISDN. The types are [Ref. 14:p. xix]: analog switch that must be replaced (Type 1), a digital switch that cannot be

upgraded to an ISDN switch (Type 2), a digital switch that can be upgraded to ISDN (Type 3), and an integrated voice/data digital switch that can be upgraded to and ISDN switch (Type 4). Within the Army, there are nine Type 1, six Type 2, 3 Type 3, and 31 Type 4 installations. This number represents 40 percent of the total 248 switches within the Army's inventory. There are 119 that are not categorized within these 99 sites [Ref. 14:p. xix]. An assessment was done regarding the deployment of ISDN within the Army. The study concluded that the Army should continue to implement LANs (to satisfy data requirements) and to replace the existing electromechanical analog switches with ISDN or ISDN upgradeable switches for the near-term [Ref. 14:p. 6-2]. This conclusion was based on several factors such as availability, cost, incompatibility, etc. However, these are only a few of the impairments that affect the Army's baseline architecture.

b. Deficiencies

Elements of the ISA baseline include Army Information Processing Centers (AIPC), Data Processing Installation (DPI), local and wide area networks, telephone systems, transmission facilities, print plants, records storage areas, office and departmental computers, PCs, visual information facilities, and libraries. The Army's long-haul communications infrastructure consists of a mixture of government-owned DCS components and leased commercial services. The baseline also contains a variety of switching systems that are subsystems of the DCS as well as the DCTN [Ref. 15:p. 3-6]. Although there are recognized deficiencies with these long-haul subsystems, the Army's baseline is concentrated heavily its on intra-base shortfalls. Most installation

communications systems are still non-integrated structures with insufficient capability and capacity for the expanding non-voice requirements. Typically, there is a telephone network which may be partially paralleled by one or more data and/or video communications systems, rather than a single integrated communications network. Furthermore, despite modernization efforts, most of the data and voice communications systems currently provided at the installation level are constrained in coping with mounting data requirements by insufficient capacity and limited interoperability. Much of the communication equipment is antiquated; still mostly using dial-up modems or dedicated circuits, obsolete or are nearing the end of their life cycle. Most of the current voice transfer equipment utilizes old key-system telephone technology, with a mix of analog, digital, and ISDN switches. The outside cable plant, primarily unshielded twisted pair, is rapidly deteriorating at some installations. Finally, many varieties of LANS are being installed in local offices and departments throughout the Army, adding to the interoperability problem. The result is a unique communications situation at each installation. The Army adds, however, that central to all of these shortfalls is the lack of a common vision for the IMA [Ref. 15:p. 3-9]. The lack of standardization, commonality and antiquated technology are major contributors to the deficiencies noted in the Army's architecture. While standards, and testing to standards, cannot resolve all of these shortfalls, it does provide a level of assurance in meeting the target architecture.

c. Target Architecture

The IMA ISA objective will be an integrated heterogeneous processing environment supporting IMA requirements. More specifically, in a quote taken from the

Executive Summary on the Army's target objective, it states that [Ref. 14:p. xvii]: "the Army's long term goal is to have a fully integrated digital communications system." The Army describes 20 objectives pertinent to meeting the overall target goal[8]:

- Reduce redundancy in systems across and within organizations, i.e., standardize and consolidate shared resources across all the disciplines
- Maximize the use non-developmental items (NDI) and COTS software, technology, and methodology
- Design and implement modern, standardized cable plants and connectivity to the end-users
- Support digitized multimedia capability, e.g., videodisc, program courseware, animation, music, etc

The Army envisions that these objectives must be satisfied through implementation of a mid-range phase (1996-2001) extended to meet the long-term goals (beyond 2001). Among some of the related mid-range target processing characteristics are: DDN, Army Standard Information Management System (ASIMS), limited dedicated lines, increase in digital usage, and a common network [Ref. 15:p. 7-8]. Relevant long-range characteristics for the communications and common network include: connectivity (DDN, ISDN, FTS-2000, partial ASIMS), interoperability, multi-level security and on-demand bandwidth. A diagram of the Army's projected architecture is illustrated in Figure 9 [Ref. 13:p. I-16]. The Army anticipates that user requirements will continue

[8]A complete list of these objectives are contained in HQ USAISC, *Information Systems Architecture, Strategic and Sustaining Base Architecture,* Volume II, December 1991, p. 4-4. Only four are listed here.

to escalate, thus complicating interoperability problems. For example, the number of telephones will remain constant at 10,000, however, the number of DTEs will increase three-fold to approximately 5200 in 1994 [Ref. 14:p. xxi]. Although progress will be made in the transition to GOSIP (which will include ISDN, FDDI, and many other standards) [Ref. 15:p. 6-8], the Army maintains that there will be a coexistence of IBM's

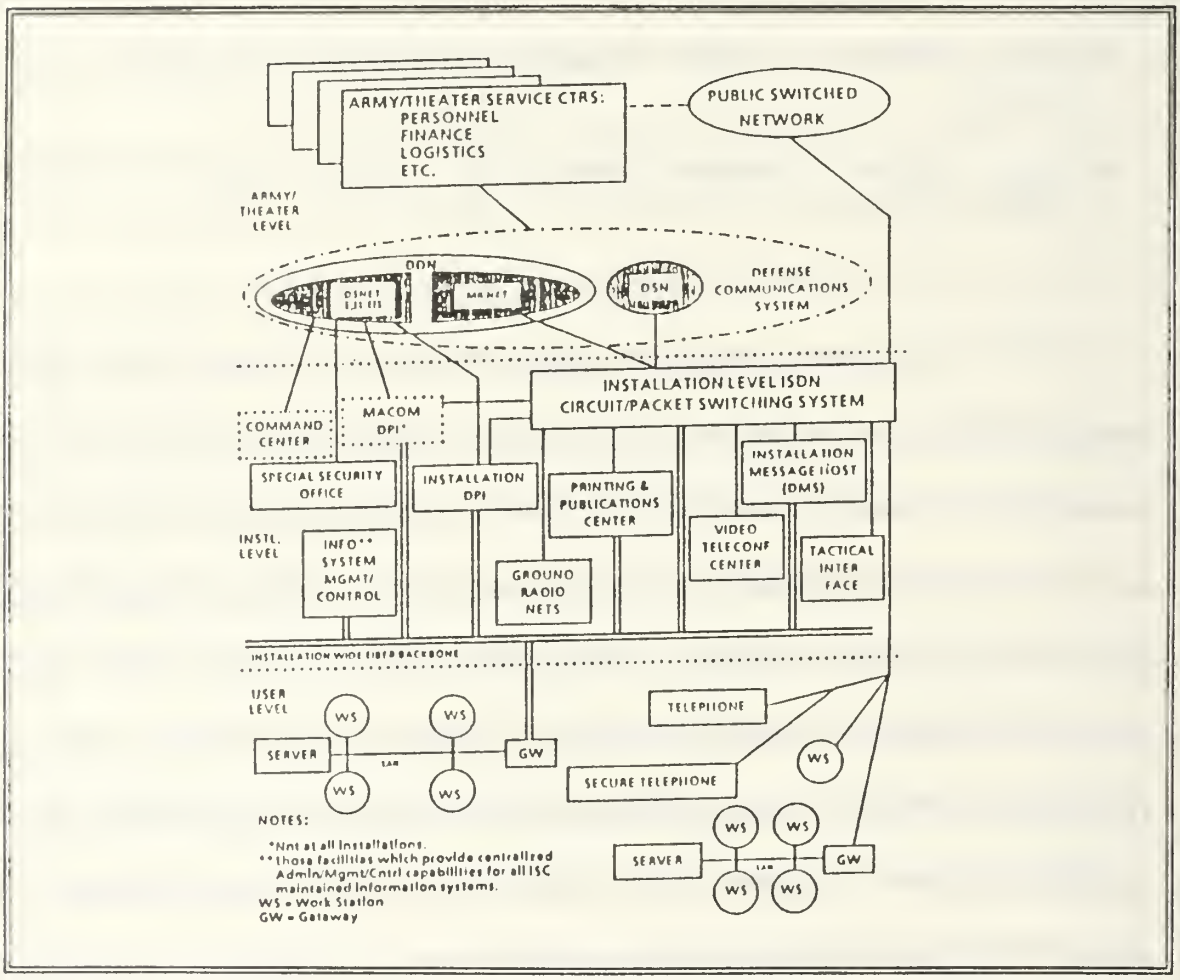


Figure 9
Projected Architecture: Systematic and Network View

Systems Network Architecture (SNA) and the current DoD protocols. The Army has taken what may be consider a reasonably good transition strategy in meeting their long-range integration targets. Their first approach is to encourage organizations to design, develop, implement, and modernize existing systems for heterogeneous interoperability, portability, and scalability. Secondly, the Army will subject new technologies to realistic tests. These test will validate and measure the ability of the technology to meet the ISA objectives [Ref. 15:p. 7-2]. This Army-wide strategy is expected to phase down vendor-dependent technologies and dependence on proprietary systems. Sharing information resources is a common theme of guidance and policy at the federal, DoD, and Army levels and is an integration goal of the Army's ISA.

All C^3 supporting network architectures involves or anticipate the use of ISDN and other evolving technologies. The Air Force is pursing ISDN installations at a rapid pace. They will migrate from the growing ISDN environment eventually to B-ISDN. The Navy is testing ISDN and have some shore sites with ISDN capabilities. Within the Base Information Transfer System (BITS) ISDN equipment is being installed at several shore locations. BITS is the basis for all new/revised intra-ship/intra-base communications network architectures and the ashore digital common user backbone. It is a subset of Copernicus[9]. They have plans to move to B-ISDN also. The Army is continuing the installation of FDDI but positioning themselves to move to ISDN with interface devices.

---

[9]Conversation between the author and Mr. Chuck Trigger, N43 Naval Computer and Telecommunications Center, Washington, DC, 20394, 3 June 1992.

III. GOVERNMENT OPEN SYSTEMS INTERCONNECTION PROFILE (GOSIP)

A. DEVELOPMENT OF OSI AND GOSIP

1. Background

Data communication between heterogeneous computer networks has become commonplace within many organizations. Historically, manufacturers and developers had a narrow view towards data communications, allowing exchange of data only with systems of similar types. This lack of flexibility later led to the development of a more universal set of data communication standards for sharing information. In the late 1960's, DARPA began a research effort, within DoD, to study and demonstrate computer resource sharing. The result was the development of what is known today as the DDN and the DoD protocol suite. The idea was to provide interoperability between organizational users to meet immediate operational needs.

However, at the same time, there has been a growing need for more robustness, modularity, greater flexibility and increased interoperability. This motivation has led to the development of the Open Systems Interconnection (OSI) standards. The OSI architecture, within the last decade, has matured and received widespread support from both vendors and users. The organization responsible for the OSI standards is the International Organization for Standardization (ISO). OSI defines and describes a common set of data communications protocols which enable systems developed by

different vendors to interoperate and enable the users of different applications on these systems to exchange information [Ref. 16:p. 5]. ISO is designed to enable heterogeneous computer systems to interoperate in a variety of data communications environments including ISDN, LANs, as well as application standards. This means that users on one host can communicate with users on another host without specific knowledge of the characteristics of the other machine. The functional components of OSI are shown in Figure 10 on the following page [Ref. 17:p. 9].

The use of the OSI standards have now been adopted by the federal government. The GOSIP, a subset of the OSI standards, is a Federal Information Processing Standard (FIPS) [Ref. 17:p. 10]. The purpose of GOSIP is to promote compatibility between government agency systems across a variety of networks. It represents a profile that is based on stable international standards developed by the ISO and the CCITT. The implementation details are based on agreements reached by vendors and users of computer networks participating in the NIST OSI Workshop. Several of the most pronounced standards-making organizations are in Appendix C. GOSIP Versions 1 and 2 have been published so far.

2. Concept

Today's information processing environment is becoming more and more reliant on networked data communications. The growing popularity of personal computers and workstations is a function of the user's ability to access data on other machines. There is also an increasing need to share information and to communicate beyond the narrow confines of a particular organization. This communication is only

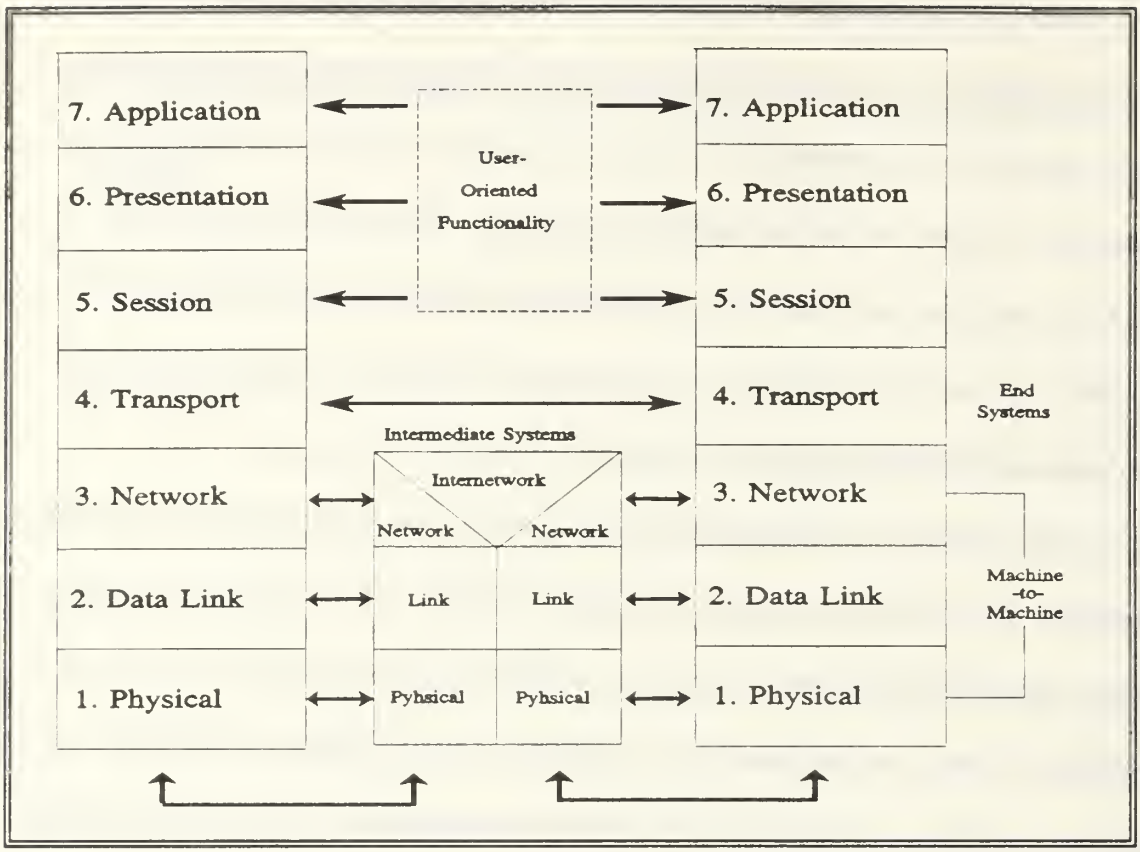
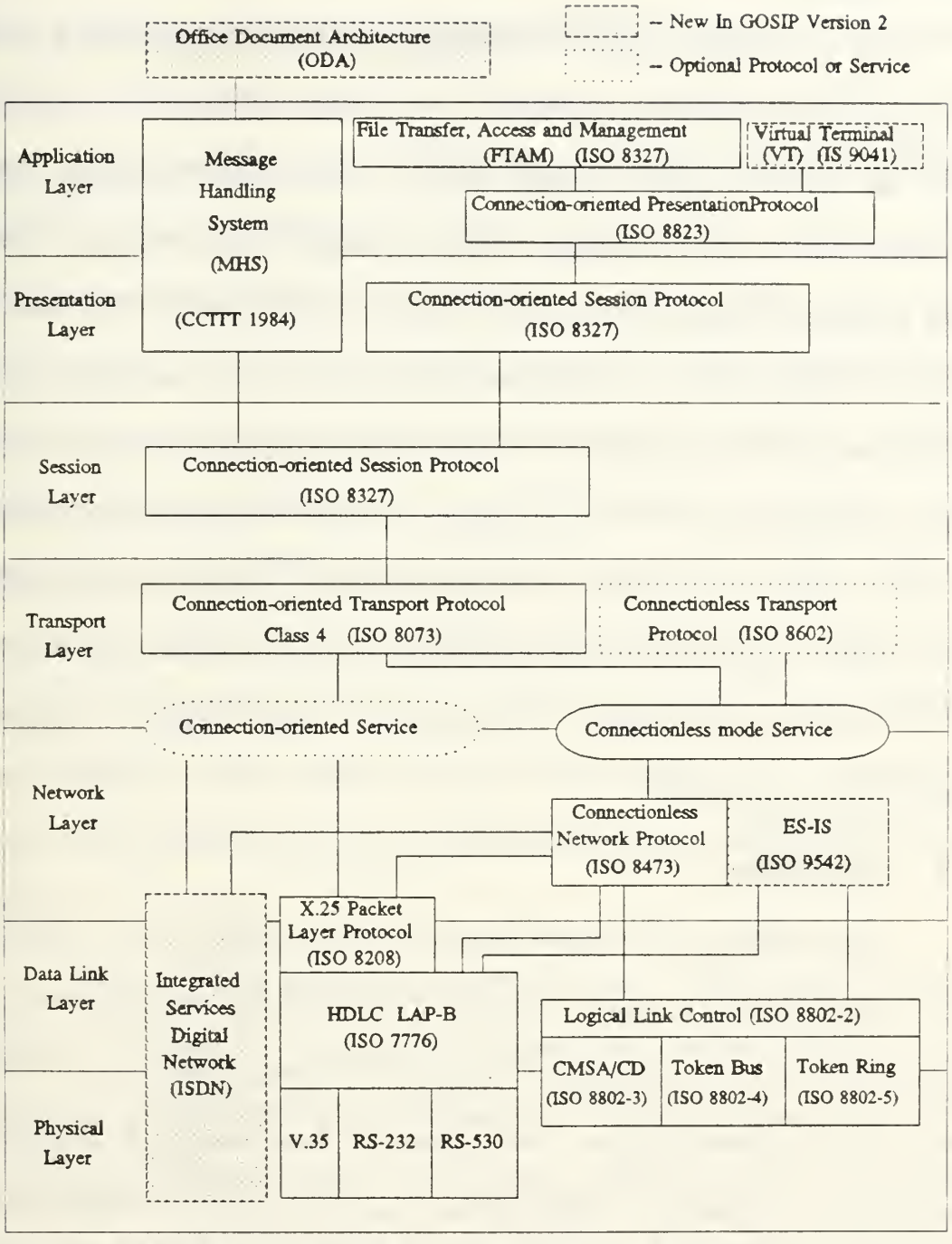


Figure 10
OSI Reference Model Layers

possible if standard protocols are developed which allow systems built by different vendors to exchange information. Much like OSI, the concept of the GOSIP is designed to meet interoperability requirements of federal agencies. Figure 11 on the next page shows the overall view of both the OSI architecture and how GOSIP uses these protocol standards [Ref. 17:p. 9]. Using the OSI as a foundation, GOSIP provides a framework upon which federal agencies should strive to meet interoperability requirements. GOSIP includes a number of OSI protocols selected from each layer of the OSI Reference Model.



* Class 0 Transport and X.25 are required for connection to public messaging systems.

Figure 11
GOSIP Version 2 OSI Architecture

3. Objective

One of the primary objectives of GOSIP is to provide a single common set of data computer and communications standards for use by federal agencies [Ref. 16:p. 7]. To meet this objective, newly acquired systems or data systems requiring major enhancements must be GOSIP-compliant. However, GOSIP does not require Federal agencies to completely replace existing data communications software. The level of commitment of agency resources to incorporate OSI products is expected not to be large over the long term. It would be possible to move to the OSI environment with minimum disruption through the use of COTS products, developed by commercial vendors. GOSIP-compliant COTS is designed to provide the flexibility, robustness, interoperability as well as reduced maintenance cost associated with in-house software development. The use of COTS products must meet any service/agency unique features or robustness desired by the C^3 environment.

4. Applicability

GOSIP applies to all federal agencies in the purchase of new networking systems or major upgrades to existing networks. The National Institute of Standards and Technology (NIST) is the organization responsible for defining open system standards for use within these federal agencies. The guidance for these standards is mandated in a variety of FIPS. Guidance for GOSIP Version 1 and 2 are published in FIPS 146 and 146-1, respectively. GOSIP Version 2, which supersedes GOSIP Version 1, establishes the mandatory compliance as of October 1992. GOSIP provides two basic capabilities.

First, it enables users to request standard applications operating over standard networks. Second, it provides a reliable end-to-end service over which users can write their own applications. The standard applications supported in Version 2 of GOSIP are File Transfer, Access, and Management (FTAM), Message Handling System (MHS), Office Document Architecture (ODA), and Virtual Terminal (VT). Standard network technologies supported include IS 8802/3 (CSMA/CD bus), IS 8802/4 (token bus), IS 8802/5 (token ring), X.25 wide area network, and ISDN. GOSIP's reliable end-to-end service allows users to exchange office documents via layers 1 through 4. The GOSIP mandate means that procurement of any computer-communications products, or major upgrades, must specify GOSIP as the single data communications standard. There are three general criteria for GOSIP applicability, as described by GOSIP Version 2 [Ref. 16:p. 28]: (1) the communication must be "computer-to-computer" (that is, between two or more intelligent systems capable of exchanging information), (2) the communicating systems must be autonomous, and (3) the communications functionality must be contained in GOSIP.

In short, GOSIP applies to procurement of new or major upgrades to existing networks. Procurement of any future computer-communications product or major upgrade must specify GOSIP as the single data communications standard. Since it deals with communications functionality, and not specific ADP configurations, it is not bound to hardware, software, or operating system limitations. This means that GOSIP may apply to all types of systems, in all types of environments. The size of the system is not

important in the context of GOSIP; neither is the communications medium used [Ref. 16:p. 28].

B. OSI ARCHITECTURE AND STANDARDS

The task of communicating in a truly cooperative way between applications on different computer is too complex to be handled as a unit. The problem must be decomposed into manageable parts. Therefore, there should be a structure or architecture that defines the communications tasks [Ref. 18:p. 446]. This line of reasoning led the ISO, in 1983, to foster the development of and adoption of a model called the OSI Reference Model. A diagram of the model is shown back in Figure 10. Some of the tenets of the OSI model, recognized by NIST, are that [Ref. 16:p. 2]: (1) each layer performs a well-defined function, (2) minimal information flows across layer boundaries, and (3) internationally standardized protocols should be "derivable" from the functionality of each layer. To reduce design complexity, the OSI architecture is organized as a series of seven layers or levels, each one built upon its predecessor. The aim of the international model is to provide a common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall reference model. Each layer offers certain services to the layers above; shielding those layers from the details of how the offered services are actually implemented [Ref. 16:p. 2]. The layering definitions provided by the OSI model is used as a framework for defining standard

protocols that can be used to implement open systems networking. Each of these layers are discussed in further in Appendix D.

In summary, the OSI model defines a framework for layered architecture, but does not provide the protocol specifications necessary to implement the network. It deals with communication functionality. Layers 1 through 3 define the machine-to-machine communications via intermediate systems. Layer 4 defines end systems-to-end system communication and layers through 7 address user-oriented functionality. The protocol processes running at any particular layer need not have detailed knowledge of processes occurring at other layers. As a result, protocol layer definitions at each layer may be modified independently.

C. DEPARTMENT OF DEFENSE (DoD) PROTOCOL MODEL AND MIGRATION TO GOSIP

In 1969, under the auspices of the DoD, the DARPA was tasked to study and demonstrate computer resource sharing. The result was the development of the DDN. The DDN now consists of a number of networks, including the MILNET, for both classified and unclassified traffic. The DDN is designed to meet the needs of DoD for both a secure command and control communications network and for ordinary unclassified communications [Ref. 18:p. 284]. An example of this is C^3 support provided by the Worldwide Military Command and Control System (WWMCCS), although the classified portion of the DDN is physically separate from the unclassified portion [Ref. 11:p. 6]. The development of the military protocol suite, often referred

to as TCP/IP, has been embraced as the defacto standard in meeting interoperability requirements. TCP/IP facilitates data interoperability between military systems worldwide. A representation of all of the DoD protocols developed for the internet is shown in Figure 12 [Ref. 19:p. 6]. Much like the OSI Reference Model, the DoD model shown in the model is based on a hierarchial or layered structure.

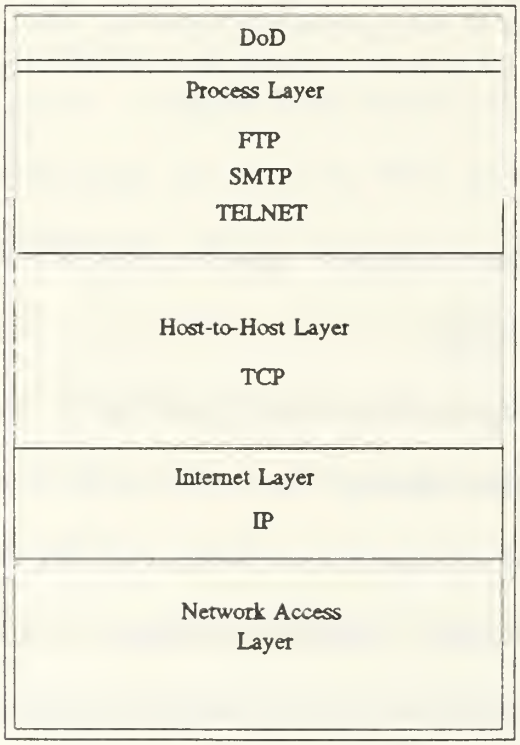


Figure 12
DoD Protocol Model

1. DoD Protocols

The Office of the Secretary of Defense (OSD) designated and reaffirmed TCP/IP, and their attendant suite of protocols, as the military standards for computer networking [Ref. 20:p. 1]. The following provides a brief overview of the DoD protocols in each layer and its use within the military.

a. Internet Protocol

The internet protocol provides the ability to interconnect various networks so that any two stations on any of the constituent networks can communicate. In general, IP is responsible for internetwork routing and delivery, and relies on network access protocols for intranetwork services. Each constituent network supports communication among a number of attached devices. In addition, networks are connected by devices that are referred to generically as gateways. Gateways provide a communication path so that messages can be exchanged between networks. IP running in a host computer accepts data in segments from TCP and sends them out across the internet and through as many gateways as needed, until they reach the intended destination. IP is sometimes referred to as "layer 3.5" of the model [Ref. 18:p. 44]. It provides unreliable connectionless service; no guarantee of delivery and packets may arrive out of sequence. However, to assure reliable data delivery, TCP must be employed.

b. Transmission Control Protocol

TCP provides a reliable mechanism for the exchange of data between processes in different computers. The protocol ensures that data are delivered error free, in sequence, with no loss or duplication. This transport service relieves higher level

software of the burden of managing the intervening communications facility [Ref. 19:p. 17]. Because the transport protocol provides for high quality service, and because it may need to deal with a range of communications services, this layer is one of the most complex of all communications protocols. TCP provides the vehicle for such basic services as electronic mail and file transfer.

c. File Transfer Protocol

File transfer protocol provides for end-user transfer of files. This may be either EBCDIC or ASCII. FTP supports both local and remote interactive or unattended file transfer. The user's communication with FTP is mediated by the operating system, which contains input/output drivers. Users on one system can retrieve files, place files, or even transfer files to a third party if access privileges are provided.

d. Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) provides for a network electronic mail facility. It provides a mechanism for transferring messages among separate systems. Users gain access to mail via a "mailbox" dedicated to them on a computer system. Through the use of these mailboxes, users can prepare messages through an editor, word processor or a COTS mail package. Since SMTP does not specify the user interface, many users are motivated to purchase COTS products to meet e-mail requirements.

e. TELNET

TELNET specifies a network standard terminal used to link users to applications; both locally as well as remotely. It is intended primarily for asynchronous

mode terminals, however, the binary transmission option allows TELNET to transparently pass any terminal traffic. This protocol allows users to interoperate with a variety of geographically disparate systems. The following table summarizes the DoD protocols and the associated MIL-STD documentation for each entity.

TABLE III-I
DOD MILITARY STANDARD PROTOCOL DOCUMENTATION

Document Name	Title	Description
MIL-STD-1777	Internet Protocol (IP)	Connectionless service for end systems across networks. Assumes an unreliable network.
MIL-STD-1778	Transmission Control Protocol (TCP)	Reliable end-to-end data transfer service. Equivalent to ISO Transport Class 4.
MIL-STD-1780	File Transfer Protocol (FTP)	A simple application for transfer of ASCII, EBCDIC, and binary files.
MIL-STD-1781	Simple Mail Transfer Protocol (SMTP)	A simple electronic mail facility.
MIL-STD-1782	TELNET Protocol	Provides a simple asynchronous terminal capability.

Both the OSI model and the TCP/IP architecture agree that the details of the intervening data transmission system should be kept hidden from the end-to-end protocols that manage communications between stations or endpoints. In the case of the OSI model, these details are handled by layers 1 - 3; for TCP/IP, a network access layer is designated. A comparison of the DoD and other protocols are shown in Figure 13 and shows the interrelationship of the functional components [Ref. 18:p. 468]. Although TCP/IP are at layers 3 and 4, many committees believe that IP is actually at layer 3.5.

The advantages of such a DoD-wide standard are interoperability, vendor productivity and efficiency, and increased competition among vendors (e.g., equipment providers) [Ref. 19:p. 3]. However, Stallings discusses several disadvantages of DoD protocols. First, they potentially inhibit innovation and other (perhaps superior) solutions. Secondly, there is a potential to limit the choices available to the customer for a specific

<table>
<tr><th>OSI</th><th>ISO</th><th>CCITT</th><th>DoD</th></tr>
<tr><td>7. Application</td><td>FTAM</td><td rowspan="2">X.400</td><td>FTP
SMTP</td></tr>
<tr><td>6. Presentation</td><td>VTP</td><td>TELNET</td></tr>
<tr><td>5. Session</td><td>ISO
Session</td><td rowspan="2"></td><td rowspan="2">TCP</td></tr>
<tr><td>4. Transport</td><td>ISO
Transport</td></tr>
<tr><td>3. Network</td><td>ISO IP</td><td rowspan="3">ISDN
X.25
X.21</td><td>IP</td></tr>
<tr><td>2. Data Link</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>1. Physical</td></tr>
</table>

Figure 13
DoD and Other Protocol Comparisons

product or functional capability. There is one other and perhaps the most important disadvantage to the DoD protocol: lack of compliance to OSI standards. Primarily

because of an immediate need to satisfy immediate operational requirements, DoD could not wait for the promulgation and vendor implementation of international standards, therefore, it does not conform to the international standards. Because of the increasingly widespread acceptance and use of these international standards, this lack of conformance places an additional implementation burden on vendors and tends to limit competition of DoD procurements. Furthermore, the international standards continue to evolve to incorporate new and more sophisticated functions and services, whereas the DoD standards are essentially static [Ref. 19:p. 4]. Regardless of additional burden, DoD has made a commitment to transition from its current use of the DoD protocols to the OSI standards.

2. Transition Strategy

A major milestone that led to development of a transition strategy was a report issued in 1985 by the National Research Council (NRC). The NRC report was the result of a study commissioned by DoD and the NIST in May of 1983. Its objective was to resolve differences between DoD and NBS on a data communications transport protocol standard. Specifically, the issue was whether or not the ISO transport standard could meet DoD's requirements instead of TCP, and, if so, how could DoD migrate to this standard. The study produced three findings [Ref. 19:p. 22]:

1. DoD objectives can be met by international standards.

2. TCP and ISO transport are functionally equivalent.

3. There are significant benefits for DoD in using standard commercial products.

It recommended that DoD migrate not only to ISO transport, but to international standards in general with cost being the major motivation. In July 1987, the policy which mandated the use of TCP/IP, was revisited by OSD. It was decided that the OSI protocols be adopted as a full co-standard with the DoD protocols and two years afterwards move to make OSI the sole mandatory interoperable protocol suite [Ref. 20:p. 47]. In fact, the DDN backbone plans to move toward complete use of the GOSIP protocols by 1993 [Ref. 16:p. 89]. The DoD strategy is to use commercial products, in preference to military standards, if they meet military requirements. The transition to the new international standards has obvious benefits. Some of these include reduced cost, increased interoperability, and increased application-level functionality. The migration to these new standards will no doubt be a challenge. Stallings believes that this process will be a slow and painful one because of the large installed base of equipment within the DoD. But one other and just as important factor is continually evolving and maturing of standards from the international communities. Efforts are being made to ensure conformance to the OSI standards and to ensure interoperability between products of different vendors. For DoD services and agencies, this means that computer networking can be done as an integration of multi-vendor, COTS components. This will be different from historical DoD TCP/IP networking for which commercial products have been widely available only recently. This easy access to vendor interoperable COTS OSI products is expected to give wider availability to networking capabilities at a reduced cost [Ref. 20:p. 1].

D. GOSIP MAJOR SUBNETWORK TECHNOLOGIES

Networks take on several characteristics and forms: star, ring, broadcast, relay, multidrop and various combinations of these. These forms can occur on any size scale, e.g., within the computer complex of a single node, around a group of adjacent nodes, or the overall system. Each form has fundamental capabilities and vulnerabilities which can affect the time required for information transfer, reliability, and security of information transfer. The selection of a specific form should be based on both the geographic distribution of nodes and expected information-flow patterns [Ref. 3:p. 168]. The harmonious coupling of diverse service-unique subnetworks make it essential to rely on a single data communications standard to support the growing integrated digital backbones. GOSIP is that single federal standard for allowing open systems communications among these diverse subnetworks in support of joint and combined operations. GOSIP identifies a number of subnetwork technology standards to allow communications on virtually any type of network infrastructure, including both local and wide area networking technologies. The following provides a general description of subnetwork technologies specified in GOSIP.

1. CSMA/CD Bus (8802/3)

A Carrier Sense, Multiple Access with Collision Detection (CSMA/CD) network consists of a series of devices connected to a cable (bus). Any device on the cable may transmit to any other device on that cable by placing the destination address on the cable along with data. The steps below describe the general operation of CSMA/CD [Ref. 16:p. 8]:

- Listen before transmitting to ensure cable is idle.
- A device begins sending a message on the cable, while at the same time "listening" on the cable and comparing what is being heard to the message it is transmitting.
- If transmission of the message completes with no discrepancy between what the device sent and what it "heard," then there was not collision and the message was successfully transmitted.
- If a collision is detected, then all transmission stops. The device (and other devices, if any, that participated in the collision) must wait, and then try again at a future time using a special "back off" algorithm.

This scheme works well for low to moderate loads (up to 40 percent), because a station may transmit with little chance of collision. For heavy loads (above 50 percent), a device waiting to transmit may be indefinitely delayed, because of the frequent number of collisions encountered. ISO 8802-3 is very close to Ethernet, although not identical. It can run on the same cable plant used for Ethernet today, even while carrying Ethernet traffic. Most vendors who have traditionally supported Ethernet now support both Ethernet and ISO 8802-3 using the same interface hardware for both. What the 8802/3-based products offer is minimal delay and reasonable throughput, particularly at low to moderate traffic loads. Additionally, CSMA/CD is fairly simple and inexpensive to implement [Ref. 16:p. 8].

2. Token Bus (8802/4)

The token bus technology, like CSMA/CD, uses a bus architecture; but here, a station needs a logical token in order to be able to transmit data on the line. Token buses are generally implemented using a broadband cable, although a baseband option

is available. This token is passed from station to station in a logical sequence (independent of the physical ordering of stations on the cable). Once the station has the token, it can send data via the bus to another station for a certain amount of time; in other words, it "seizes" control of the bus for a predefined time interval. When that time expires, the station relinquishes the token. [Ref. 16:p. 8].

3. Token Ring (8802/5)

A token ring network consists architecturally of a number of stations connected to one another via a circular cable or loop. A token travels around the ring; this token confers on a station the ability to send data. When a station wants to send, it looks for the free token; if it is available, it grabs the token, changes it to a "busy" token, and appends data to it. The data travels around the ring to the destination station(s). When the data has been received by the sending system, it is removed from the ring. After a station has finished transmitting the last bit of data, it must regenerate the free token [Ref. 16:p. 8]. ISO 8802-5 implements the IBM token ring technology. It allows GOSIP-compliant systems to run over the same cable plant used for IBM token ring installations. GOSIP systems and IBM systems may even share the same ring. However, GOSIP systems will only be able to communicate with other GOSIP systems, because the upper layer protocols must match for communications to occur [Ref. 17:p. 23].

4. X.25 Wide Area Networks (WANs)

For transmission over long distances, existing public network facilities are often used. Since there are so many types of devices that could be attached to such facilities, the X.25 protocol was developed for network access. CCITT X.25 is the international standard for public switched packet data networks (PSDPNs). It defines a standard interface between a DTE and data circuit-terminating equipment (DCE) [Ref. 16:p. 60]. To support this type of interface, X.25 protocol establishes a virtual circuit between two devices; this is a definite path connecting the two machines through intermediate machines. This path is valid for the duration of the connection. Source and destination addresses, as well as other information, are put on a call request packet; data packets follow. The 1984-based X.25 protocols offer enhanced capabilities from the 1980 Recommendation to support OSI applications, such as Network Layer addressing and quality of service provision. GOSIP requires 1984 X.25 in Version 2. While X.25 is usually orders of magnitude slower than typical local area networks, it does not have any distance limitations. X.25 service is offered by numerous vendors in the U.S.

5. Integrated Services Digital Network (ISDN)

ISDN is the newest subnetwork technology to be included in GOSIP Version 2. ISDN offers the advantages of (1) cost control (e.g. controlling access to the network), (2) high capacity (up to 100 times the data rate of conventional networks), and (3) flexibility (due to its ability of simultaneously transmitting voice, data and video from a single instrument) [Ref. 16:p. 8]. Architecturally, ISDN is layered in the same fashion

as the OSI Reference Model, although many ISDN protocols describe different functionality than that described by the OSI protocols belonging to the same layer. Figure 11 back on **page ?**, illustrates how ISDN, as a subnetwork technology, fits into the overall OSI Reference Model. GOSIP references two combinations of channels on the ISDN digital pipe: (1) basic rate, which provides a minimal level of capability, and (2) primary rate, which provides an expanded set of capabilities over the basic rate. Chapter IV provides in-depth details of ISDN. Regardless of the standards being developed, incompatibilities still exist between ISDN switches of different manufacturers and between ISDN switches and terminals. The interpretation of the evolving standards by the developers is one of the major cause of these incompatibilities.

6. Local Area Network Bridges

Local area network (LAN) bridges are devices that connect LANs of the same type. The bridging occurs at the Data Link Layer (Media Access Control) and is therefore transparent to the systems attached to the LANs; the bridged LANs appear to operate as if they were a single subnetwork, with messages transmitted on one LAN being automatically transmitted on the other by the bridge. Currently, bridges between 8802/3 local area networks are on the rise. The GOSIP FIPS does not explicitly reference LAN bridges (or specifications), but their use is not precluded as long as their use does not compromise GOSIP LAN functionality [Ref. 16:p. 60]. On top of a lower layer technology, GOSIP mandates the use of the connectionless network layer protocol, Transport Protocol Class 4 (TP-4), and the session protocol. Transport Protocol Class 0 (TP-0) and the Connection Oriented Network Service (CONS) are mandated only in

conjunction with public data network messaging (e.g. Message Handling Systems). The provisions of the CONS, for general use, and the Connectionless Transport Protocol (CLTP) are options that may be specified in addition to the GOSIP mandatory Connectionless Network Service (CLNS) and Transport (class 4), respectively.

E. END-TO-END PROTOCOL CONSIDERATIONS

The subnetwork technologies specified within GOSIP suggest several means by which to support user applications. Two specific layers are used to interconnect the many user applications over a variety of disparate networks: transport and network layers.

1. Transport Layer

The transport layer is a layer 4 service that provides the means to establish, maintain and release transport connections on behalf of session entities [Ref. 22:p. 175]. Within ISDN, this layer is used for end-to-end user signalling on the D-channel. The transport layer provides reliable, transparent transfer of data between end points and end-to-end error recovery and flow control. In essence, it ensures that packets are delivered error-free, in sequence, with no losses or duplications. GOSIP specifies two types of services available from the transport layer--connection-oriented and connectionless. These are referred to as the Connection-Oriented Transport Protocol (COTP) and the Connectionless Transport Protocol (CLTP). They are distinct services and are used for different circumstances.

a. Connection-Oriented Transport Protocol (COTP)

This protocol provides a reliable, orderly end-to-end data transfer which is analogous to transfer of a pre-fabricated house. Each piece is moved from one state to a new state and reassembled properly with no damage having incurred in transit. With connection-oriented transport service, data packets are received in the correct order by the end user. Many parameters are negotiated between two communicating transport entities. These provide proper flow control, proper sequencing, and proper error detection and retransmission of lost data. ISO provisions five transport services (TP-0 through TP-4). TP-4 assumes the least about network layer services and is required for GOSIP systems. One domain in which this service is employed is the MHS. CCITT mandates that TP-0 and the Connection-Oriented Network Service (CONS) be used by end systems when messaging over public messaging domains on public data networks. All end systems on private management domains must use TP-4. Transport Class 2 (TP-2) is used in conjunction with the connection-oriented network service. It is designed for use with CONS where communications is confined to a single logical subnetwork. Although TP-2 is used in some government applications, TP-4 will remain the sole mandatory data transport service for purposes of interoperability among GOSIP-compliant systems.

b. Connectionless Transport Protocol (CLTP)

This protocol is used to provide the Connectionless Transport Service (CLTS). The CLTP is to used only as an option among participants with a similar capability. Although there are no NIST/OSI Workshop implementation agreements on

CLTP presently, the CLTP is included so that non-OSI applications can take advantage its services. For example, it is possible to run non-OSI applications, such as the Network File System (NFS), using CLTS [Ref. 16:p. 6].

2. Network Layer

The function of the network layer is to relay and route network service user packets to the correct destination, while as the same time masking the differences in the underlying subnetwork technologies (e.g., X.25, Token Ring, ISDN). It relieves the transport layer of the need to know anything about the underlying data transmission and switching technologies used to connect systems [Ref. 19:p. 186]. The network service establishes, maintains and terminates connections between communications facilities. The network layer, like the transport layer, also offers both connection-oriented and connectionless services.

a. Connectionless Network Service (CLNS)

The Connectionless Network Service (CLNS) is provided by the Connectionless Network Protocol (CLNP). It allows different GOSIP subnetworks to interconnect as transparent OSI network entities (e.g., X.25 and ISDN). The CLNP masks the differences between these subnetwork technologies and allows these differences to be transparent to the OSI Network Layer user. Since the protocol is connectionless, each protocol data packet is routed separately and the header contains addressing information as well as information relating to the optional service provided by the protocol (e.g., priority and security). This could significantly decrease throughput in intermediate systems [Ref. 16:p. 7]. GOSIP Version 1 originally required that the

processing of packets by the CLNP be in order of priority. However, because of the potential significant loss of throughput in intermediate systems, it was deleted from GOSIP Version 1. The services of existing subnetwork technologies must be augmented to provide the OSI Network Layer service; this enhancement is also provided in the CLNP. NIST states that work is in progress to allow the CLNP and the Connection-Oriented Network Service (CONS) to interoperate. The End-System (ES)-to-Intermediate System (IS) routing protocols have now been specified in GOSIP Version 2 to provide the capability for hosts (end systems) and routers (intermediate systems) to locate one another. This eliminates the need for some static configuration information and permits host to be moved without reconfiguration [Ref. 23:p. 4].

b. Connection-Oriented Network Service (CONS)

While CLNP is a mandatory GOSIP requirement, the use of CONS has been specified as an optional service. Use of CONS can improve efficiency of the network layer when operating over a single logical connection-oriented subnetwork (e.g., a single X.25 subnetwork, a set of X.25 networks interconnected by X.75 devices, or an ISDN) [Ref. 16:p. 7]. Use of this service can, under certain circumstances, avoid the overhead associated with the CLNP and may permit interoperability with end systems that do not implement the connection-oriented protocol.

F. GOSIP SECURITY CONSIDERATIONS

Confidentiality, data integrity, access control, non-repudiation, and user authentication are among several concerns of military organizations. There are also

increasing threats to computer networks today, like viruses, that make these systems highly vulnerable to attack. Military systems using OSI protocols will need to incorporate protection mechanisms to control access and information exchange [Ref. 24:p.6]. The OSI Security Architecture is an International Standard (IS 7498/2) and was adopted in 1988. Figure 14 depicts the security architecture which has been superimposed over the OSI Reference Model [Ref. 21:p. 45]. The security architecture suggests a range of choices for security services and their placement. The standard describes a general architecture for OSI security, defines a set of security services that may be supported within the OSI model, and outlines a number of mechanisms than can be used in providing the services [Ref. 21:p. 26]. The OSI Security Architecture provides a basis for developing security and defines several primary security service requirements that can be implemented at one or more layers of security model. A summary of these security services are summarized below [Ref. 21:p. 42]:

- Data confidentiality services protect against unauthorized disclosure. Protecting the details of an attempted corporate takeover is an example of the need for confidentiality.
- Data integrity protect against unauthorized modification, insertion and deletion. Electronic funds transfer between banks is where this type of service is warranted.
- Authentication services verify the identity of communicating peer entities and the source of data. Owners of bake accounts require assurance that money will be withdrawn only by the owner.
- Access control services allow only authorized communication and system access.
- Non-repudiation with proof of origin provides to the recipient proof of the origin of data and protects against any attempt by the originator to falsely deny sending the data or its contents.

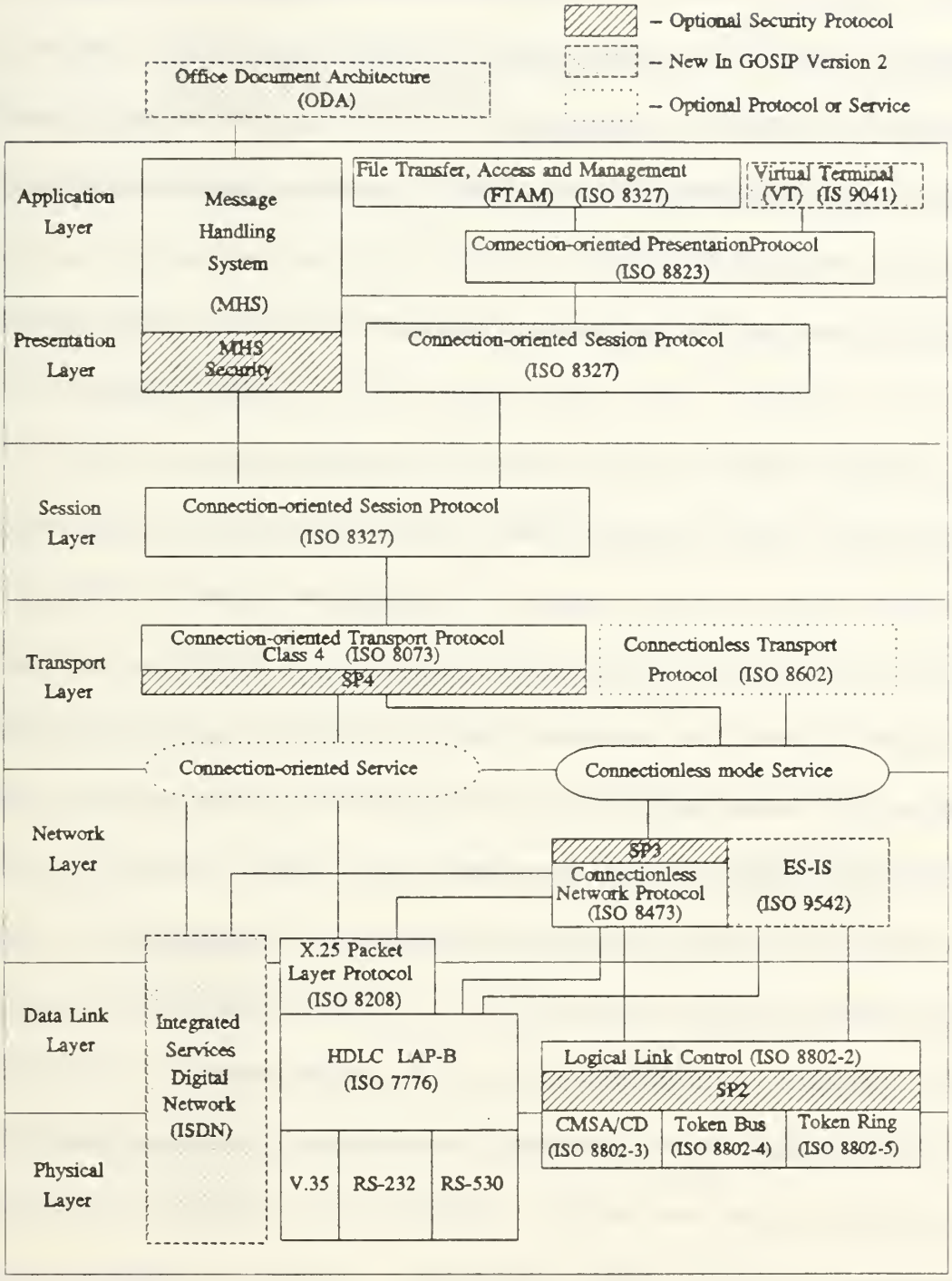


Figure 14
Framework for OSI Security

The security architecture, however, does not provide specifications for implementing security; no protocols, formats or minimal requirements. To provide robust security specifications, a significant level of effort is required that can be used in standards. Secure Data Network System (SDNS) is one effort under development to provide robust security specifications.

SDNS is an example of implementing the required security in accordance with the OSI Security Architecture. The premise behind SDNS is to serve as the basis for protecting classified data as well as unclassified, but sensitive, data in a wide range of applications [Ref. 16:p. 71]. It incorporates a set of security protocols and procedures that provide a number of security services of the OSI Reference Model. SDNS can be used in a variety of networks including local area networks, wide area networks and point-to-point communications networks. It offers comprehensive security in a number of network applications including electronic message handling and file transfers. GOSIP specifies that security services may be provided at one or more of the layers 2, 3, 4, 6, and 7. However, for SDNS, protocols and procedures for providing specific security services are being developed at layers 3, 4 and 7. Specifications for security at layers 3 and 4, specifically, are included within the SDNS project sponsored by NIST [Ref. 21:p. 43]. Additionally, specific algorithms for confidentiality, integrity, authentication, and key distribution have been specified. GOSIP Version 2 addresses limited security implementation capabilities at the network layer. However, additional security enhancements are a future service for inclusion in GOSIP Version 3 [Ref. 21:p. 41] as well as inclusion in FIPS, ANSI, and ISO standards.

G. FUTURE GOSIP RELEASE VERSIONS

New versions of GOSIP will be issued no more frequently than once a year and the comments of manufacturers, government agencies and the public will be solicited before each new version is released. Protocols will be mandated for use in federal procurements initiated one year after the effective date of future version in which they are included or approximately 18 months after that version is promulgated as a FIPS.

1. GOSIP Version 3

The future release of GOSIP Version 3 will be issued in conjunction with federal, Manufacturing Automation Protocol (MAP), Technical Office Protocol (TOP), and Electric Tower Industry standards in a common document called the Industry Government Open Systems Specifications (IGOSS). The IGOSS represents a corporate effort by industry, private and government organizations to provide commonality within the development of open systems. GOSIP Version 3 will point to the IGOSS and much smaller than previous releases. The version will contain a "Federal Applicability Statement" mandating specific government requirements and will contain any protocols not agreed to by the four organizations. IGOSS will be released in draft form in September 1992. The final version is expected to be released in the Spring 1993[10]. The following protocols are candidates for inclusion in Version 3 of GOSIP [Ref. 21:p. 41]:

---

[10]Telephone conversation with Mr. Jerry Mulvena, NIST, Manager, Network Applications Group, Gaithersburg, Maryland, 5 June 1992.

- Directory Services
- Optional Class 2 Transport Protocol
- Computer Graphics Metafile (CGM)
- Virtual Terminal (X3, page, scroll profiles)
- MHS extensions based on 1988 CCITT Recommendations
- FTAM extensions
- Fiber Distributed Data Interface (FDDI)
- Network Management (Also the subject of a separate FIPS)
- Optional Security Enhancements
- SGML (Standard Generalized Markup Language)
- Manufacturing Message Specification
- Intra-domain Dynamic Routing

2. GOSIP Version 4

The following protocols are candidates for inclusion in Version 4 of GOSIP [Ref. 21:p. 41]:

- Transaction Processing
- Remote Database Access
- Additional Optional Security Enhancements
- Additional Network Management Functions
- Inter-domain Dynamic Routing

IV. DATA SERVICES USING INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

ISDN, in general, evolved from a telephony IDN and is based on circuit-switched technology [Ref. 26:p. 73]. It was contrived to provide a global, efficient, flexible, and cost effective end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard user-network interfaces. Its aim is to integrate existing services and new technologies into a single network interface. Some of the ISDN benefits include integrated voice, data, fax and high-resolution graphics, emerging multimedia applications, and even video programming and conferencing. ISDN can also be used effectively to interconnect local area networks. Figure 15 on the following page illustrates the basic structure of an ISDN network [Ref. 27:p. 4].

GOSIP Version 2 addresses only the data communication aspects of ISDN as provided by CCITT X.31 (Support of Packet Mode Terminal Equipment by an ISDN). Therefore, only a small subset of the ISDN technology is required under GOSIP. ISDN will provide an alternative subnetwork technology for GOSIP end-systems and function as an intermediate subnetwork between other subnetwork types [Ref. 16:p. 2].

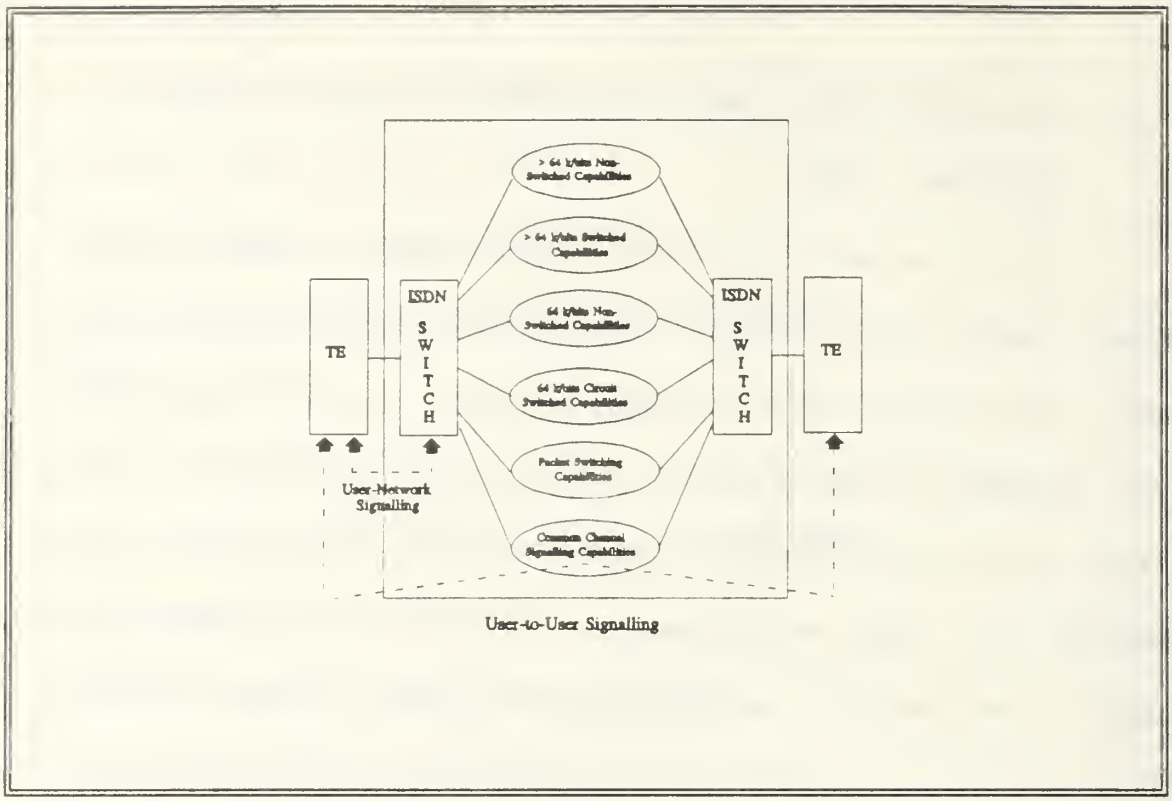


Figure 15
Basic ISDN Architectural Model

A. ISDN CONCEPT AND OBJECTIVE

1. Concept

The concept of ISDN is to provide an economic voice and data transmission mechanism over an integrated interface. Instead of a large number of interfaces (telephone network, telex, specialized data networks, leased lines, etc), ISDN will provide a single interface to the network. A key element of service integration for an ISDN is the provision of a range of digital services using a limited set of connection types and multi-purpose user-network interface arrangements. Access to these services

is standardized and according to the CCITT recommendations. The aim of the standard digital approach is to support a variety of applications over both circuit- and packet-switched connections. ISDN offers a meaningful way of providing access to multimedia services without the overhead of individual circuits or proprietary technology. Figure 16 shows a users conceptual view of ISDN [Ref. 18:p. 704].

2. Objective

The need to provide communications between the numerous islands of automation and geographically diverse networks has been a major focus of many standards committees. One desire for switched digital services is at speeds greater than the conventional 56 kbps now available. Activities currently under way has led to the development of a worldwide ISDN to provide the functionality needed by users. This effort involves national governments, data processing and communications companies, standards organizations, and other communities. The development of any standard, however, requires the consensus of all such organizations. While the standards are still evolving, these disparate groups share the same ISDN objectives. Some of the key objectives promoted by these groups are described by Stallings [Ref. 18:p. 70]: (1) standardization, (2) transparency, (3) separation of competitive functions, (4) leased and switched services, (5) cost-related tariffs, (6) smooth migration, and (7) multiplexed support. Of these objectives, probably the most important ones are standardization and transparency. A single set of ISDN standards provide universal access and permit development of cost-effective equipment in support of ISDN services. Transparency in transmission permits users to develop applications and protocols with confidence that they

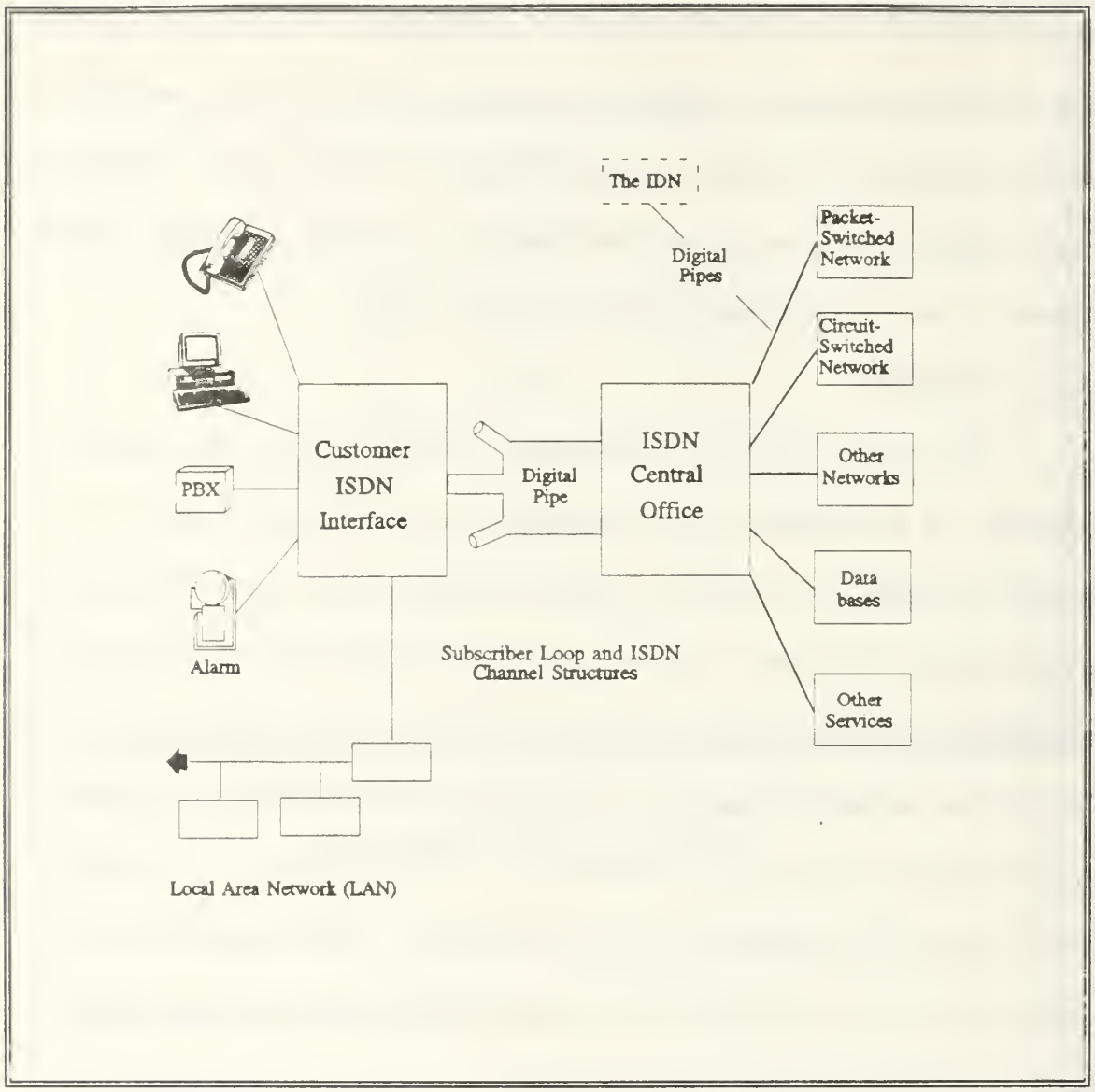


Figure 16
Conceptual View of ISDN

will not be affected by changes in the underlying ISDN technology. Collectively, these objectives establish a baseline upon which to ensure interoperability of ISDN in a multi-vendor environment.

B. ISDN RELATIONSHIP TO OSI

1. ISDN and the OSI Reference Model

The OSI Reference Model is one of the most important concepts in data communications. This model serves as the framework within which communications protocol standards are developed and as a frame of reference for addressing data communications [Ref. 25:p. 377]. The relationship between ISDN and the OSI Reference Model is described, at best, as extremely difficult in showing a precise correlation because there are certain requirements for ISDN that are not met within the current structure of OSI. This conclusion is shared by both the DoD, (Military Standards 188-194), and by Stallings [Ref. 25:p. 27]. GOSIP Version 2 further concludes that, although ISDN is layered in the same fashion as the OSI Reference Model, many ISDN protocols delineate dissimilar functionality than that described by the OSI protocols belonging to the same layer [Ref. 16:p. 10]. The reason for the difficulty in showing a clear relationship is based partly on several of the ISDN characteristics:

- The use of out-of-band signalling. An example is the use of the D-channel which is used to set up, maintain, and terminate a connection on the B-channel. [Ref. 28:p. 26]
- Multimedia calls. ISDN will allow a call to be set up that allows information flow consisting a multiple types, such as voice, data facsimile, and control signals [Ref. 25:p. 276].
- Multipoint connections. ISDN will allow conference calls [Ref. 25:p. 276].

2. ISDN Protocol Structure

The evolution of standards for ISDN includes the development of protocols for interaction between ISDN users and the network, and for interaction between two ISDN users. Although there are differences in the ISDN requirements and the OSI structure, Figure 17 attempts to show some correlation of the OSI and ISDN layers [Ref. 25:p. 276]. As a network, ISDN is essentially unconcerned with layers 4 - 7 of the model. These are end-to-end layers employed by the user for the exchange of information. Layer 1 specifies the physical interface for both basic and primary access. With this physical configuration, both the B and D-channels are multiplexed over the same physical interface. The D-channel supports control signalling, packet-switching, and telemetry (for some low speed applications) and is always present to support a user's request. The layered protocol structure used by the B-channel differs greatly from the D-channel. The B-channel can be used to provide circuit switching, semipermanent circuits, and packet-switching service. When the B-channel is used in circuit switching and semipermanent technologies, the D-channel is used to set up a full-duplex, transparent circuit (data transfer) between two ISDN users. Users are free to use their own formats, protocols, and frame synchronization. Hence, from the point of view of ISDN, layers 2-7 are not visible nor specified (Figure 17). With packet-switching service, a circuit-switched connection is set up on the B-channel between the user and a packet-switched node using the D-channel control protocol. Once the circuit is set up on the B-channel, the user employs X.25 at layers 2 and 3 to establish a virtual circuit to another user. The packetized data is then exchanged over the B-channel. Above the

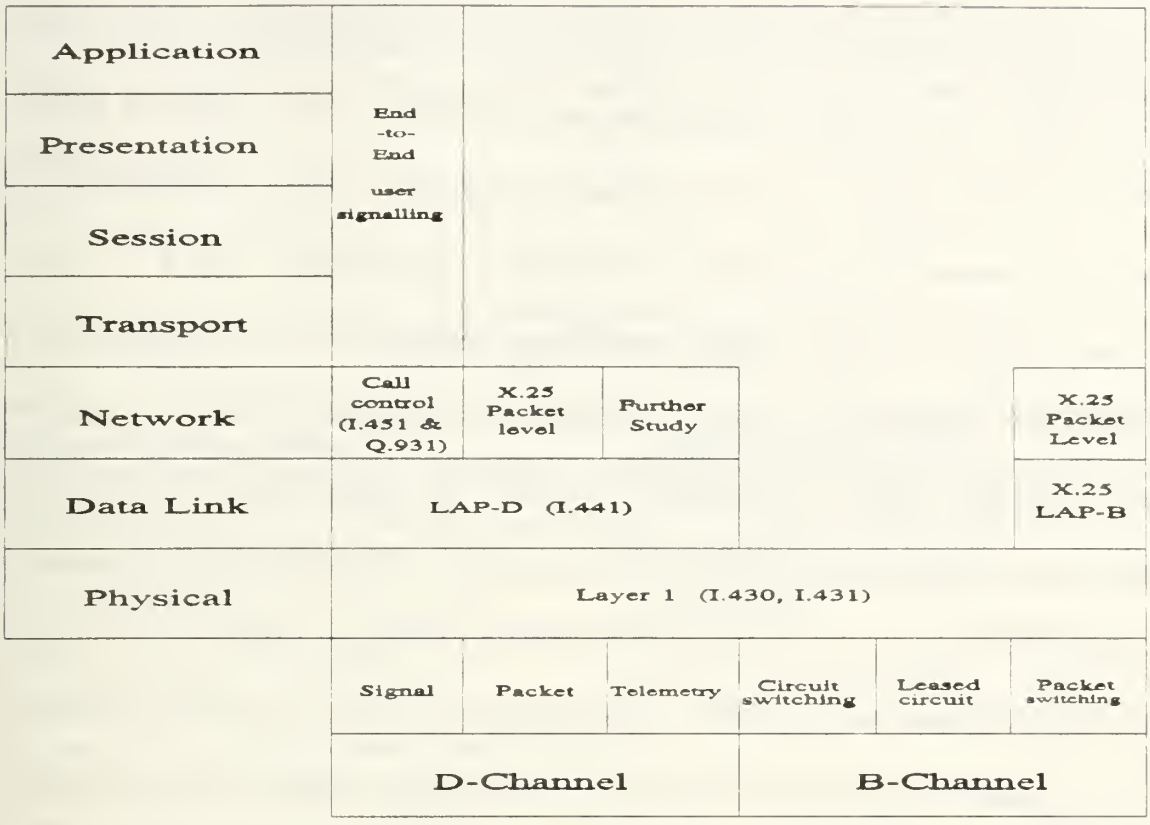


Figure 17
Layered Protocol Structure

network layer, the protocol structure differs for the two channels. Further discussion of the D- and B-channels are detailed in the next section.

C. ISDN STANDARDS AND FEATURES

ISDN is an end-to-end digital service providing a wide range of connection-oriented voice, data, video, and other services. It provides an alternative to X.25 data networks as a connection-oriented subnetwork over which OSI protocols may be used [Ref. 23:p. 46]. The development of ISDN is governed by a set of guidelines called the I-series of

recommendations and the Q-series is in support of control signalling such as SS7. Most of the CCITT I- and Q-series recommendations for ISDN have been adapted to North America and promulgated as American National Standards. Should a conflict occur, these ANSI standards take precedence over the CCITT standards [Ref. 14:p. 3-9]. Like other networking technologies, ISDN standards are still evolving both nationally and internationally. There are a number of standards organizations involved in various aspects of ISDN. Within the United States, the NIST has organized the NIU-Forum to address two specific problems within the ISDN arena [Ref. 23:p. 46]: (1) interoperation between ISDN switches, and (2) definition of protocol profiles for ISDN services (e.g., point of sale terminals and fax). The result of this work is the publication of the NIU-Forum Agreements on ISDN which provides the development status of implementation agreements, conformance tests, and application profiles. The next four sections describes some of services, standards and features of ISDN.

1. Bearer Services and Teleservices

Bearer service is a particular type of technical and operational service that provide circuit- or packet-switched transport of information between two terminal-network interfaces irrespective of the compatibility of the terminals. A typical example of these services are switched or non-switched 64 kbps B-channels for text, data and graphic applications [Ref. 26:p. 76]. The primary requirement for ISDN in GOSIP is as a network bearer service accessible via terminal and switching equipment that can be connected readily, regardless of the specific vendor. Bearer services provide the means to convey information (e.g., speech, data, video, etc.) between users in real time without

alteration of the message content. CCITT defines 12 different bearer services for use by ISDNs. The table below delineates these services for both circuit- and packet-modes [Ref. 25:p. 189].

TABLE IV-1
ISDN BEARER SERVICES

Circuit-Mode Bearer Services	Packet-Mode Bearer Services
64 kbps, 8 KHz structured, unrestricted	Virtual call and permanent virtual circuit
64 kbps, 8 KHz structured, speech	Connectionless on a D-channel
64 kbps, 8 KHz structured, 3.1 KHz audio	User signalling
64 kbps, 8 KHz structured, alternate speech/unrestricted	
64 kbps, 8 KHz structured, alternate speech/3.1 KHz audio	
384 kbps, 8 KHz structured, unrestricted	
1536 kbps, 8 KHz structured, unrestricted	
1920 kbps, 8 KHz structured, unrestricted	
2 x 64 kbps, 8 KHz structured, unrestricted	

The 64 kbps, 8 kHz structured, unrestricted is the most general purpose service. The 8 kHz means that, in addition to bit transmission, a structure is transferred between customers. "Unrestricted" implies that the information is transferred without alteration and is known as a transparent bearer services. [Ref. 25:p. 190] The bearer services listed in the table above are the minimal set of bearer services which are to be supported by public networks for ISDN basic rate (ANS T1.604-1990) and primary rate

interfaces (ANS T1.603-1990). These services conform closely to CCITT architectural concepts and describe the constraints in the U.S. telecommunications environment for the ISDN basic and primary rate interfaces.

In addition to the bearer services provided by ISDN, teleservices are also supported. Teleservices build upon the bearer services and include integrated voice, image, data, and video. These type services correspond to layers 4 through 7 of the OSI model and usually referred to as the user access part of the ISDN functional architecture. While bearer services define requirements for network functions, teleservices include terminal as well as network capabilities.

2. Physical Layer Standards

GOSIP does not mandate a specific physical interface standard for connecting devices at the lowest layer. However, there are three interfaces most commonly used and recommended in conjunction with X.25: (1) EIA standard RS-232-C, for line speeds up to 19.2 kbps, (2) CCITT V.35 for line speeds above 19.2 kbps, and (3) EIA RS-530 for transfer rates above 20 kbps. For narrowband ISDN, the physical layer specifies both a basic rate and a primary rate interface. The physical interface at this level is usually an RJ-45 modular jack/plug. The same interface is designed to be usable for telephone, computer terminal, and videotext terminals. This common physical interface provides a standardized means of attaching to the network.

a. Basic Rate Interface (BRI) Services

The BRI, the lowest layer of ISDN, provides a 16 kbps signalling D-channel and up to two 64 kbps B-channels. The total bit rate of the basic rate access is

192 kbps which includes framing, synchronization, and other overhead bits. BRI allows simultaneous use of voice and multiple data applications, such as packet-switched access, a link to a central alarm service, facsimile, teletex, and more. Some of the key characteristics of the BRI is that it provides (1) encoding for transmission, (2) framing for multiplexing and, (3) contention resolution for multidrop configurations [Ref. 25:p. 281]. Figure 18 shows a general illustration of the basic rate access services offered by an ISDN [Ref. 28:p. 27]. Although a Network Termination 2 (NT2) device is shown in the figure, NT2 equipment is more likely to be used in the PRI environment than in a BRI configuration.

Each reference point at the BRI defines a conceptual point at the conjunction of two non-overlapping functional groupings. Functional groupings are certain finite arrangements of physical equipment or combinations thereof. These reference points are identified as R, S, T, and U as shown in Figure 18. Reference point U (user) describes the full-duplex data signal on the subscriber line. Reference point T (terminal) corresponds to a minimal ISDN network termination at the customer's premises and separates the network provider's equipment from the user's equipment. Reference point S (system) corresponds to the interface of individual ISDN terminals. It separates users terminal equipment from network-related communications functions. Reference point R (rate) provides a non-ISDN interface between non-compatible ISDN user equipment and adapter equipment. The two types of subscriber equipment defined for use with ISDN are terminal equipment type 1 (TE1) and terminal equipment type 2 (TE2). TE1's are devices that support the ISDN standard interface and may include

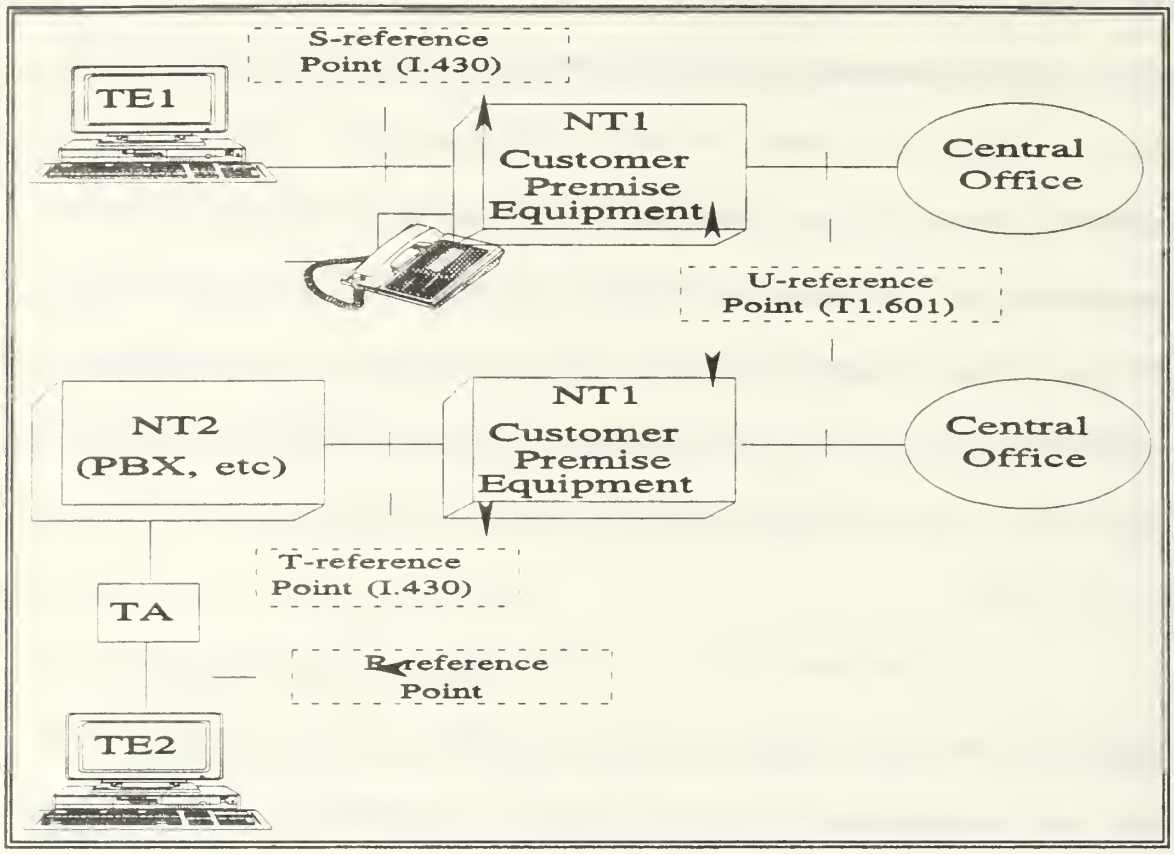


Figure 18
Basic Rate Interface (BRI)

digital telephones, integrated voice/data terminals, digital facsimile, etc. TE2's represent non-ISDN compatible equipment. They might include personal computers, printers, other RS-232C connections or X.25 interface equipment [Ref. 25:p. 245]. Equipment of this type requires a terminal adapter (TA) which allows non-ISDN devices to interface to an ISDN. Terminal adapters perform rate adaption of conventional low speed equipment (e.g., RS-232 devices) to ISDN. Adapters also convert out-of-band control signalling to in-band signalling and vice versa. Although GOSIP Version 2 suggests direct ISDN connectivity of computer devices, terminal adapters will be allowed to

accommodate non-ISDN devices [Ref. 16:p. 2]. The NT1 equipment shown in Figure 18, includes functions associated with the physical and electrical termination of the ISDN on user's premises. NT1's performs line maintenance (e.g., loopback testing and performance monitoring. They may be controlled by the ISDN provider to isolate the user from the subscriber loop. The basic rate access is by far the most widely used. It is designed to meet the needs of most individual users not requiring high-speed graphics. Currently, there are approximately 200,000 installed BRI lines in the United States [Ref. 29:p. 44] and this growth can be expected to continue well into the next decade.

b. Primary Rate Interface (PRI) Services

The PRI, also at the lowest ISDN layer, provides one 64 kbps signalling D-channel and up to twenty-three (23) 64 kbps B-channels. It uses a 2-wire pair to provide data rates of 1.544 Mbps, which when framing overhead (8 kilobits) is subtracted, it actually becomes 1.536 Mbps. A generic physical configuration of a PRI is illustrated in Figure 19 on the next page [Ref. 28:p. 28]. The basic interface will be used at the S, T, and U reference points and the primary interface at the U reference point [Ref. 22:p. 13]. The NT2 equipment shown, usually refers to customer premise equipment (CPE) such as a private branch exchange (PBX). It could also be a terminal controller or a LAN. In the sense of a PBX, NT2 provides private or additional features not ordinarily offered by a central exchange office. This might include a 4-digit dial plan or local data exchange services. This primary rate access is intended for users with high capacity requirements such as high resolution graphics or imaging. It uses the current T-1 based technology and follows CCITT Recommendation G.703 [Ref. 28:p. 28].

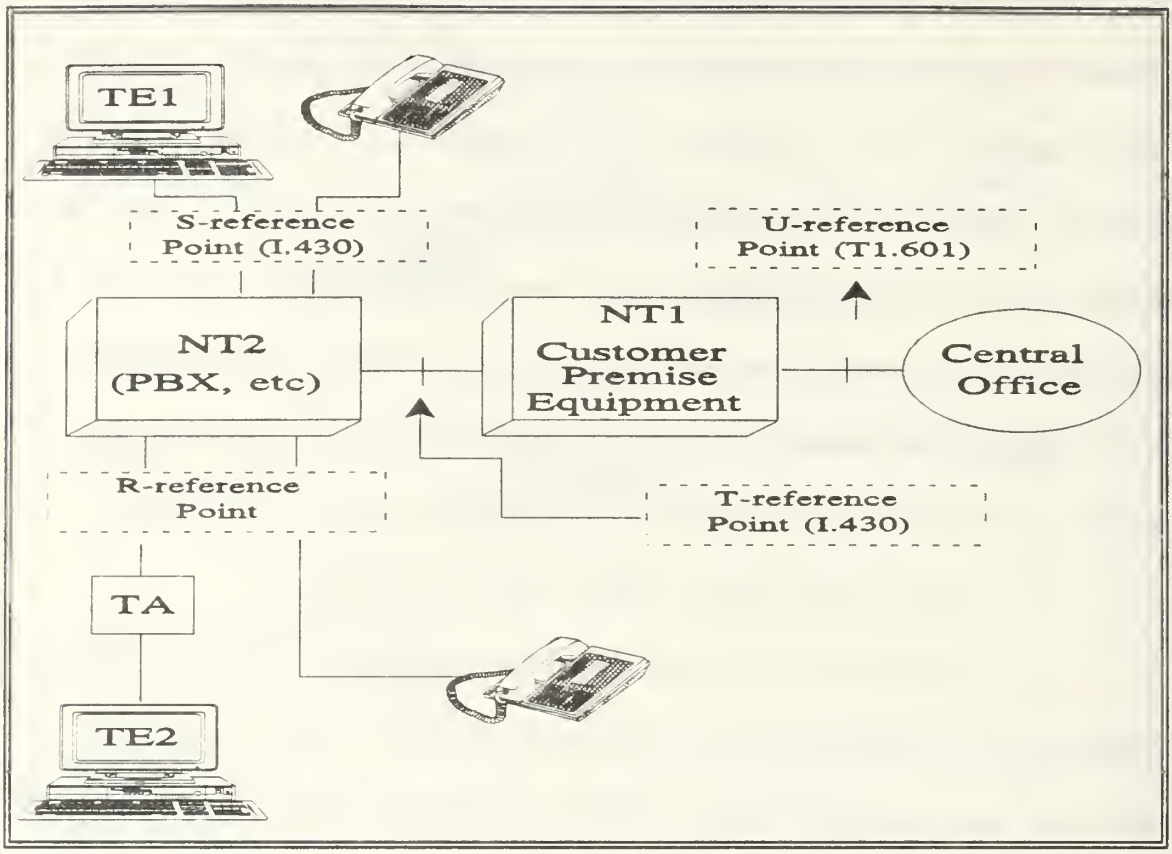


Figure 19
Primary Rate Interface (PRI)

However, unlike T-1, individual B-channels can be dynamically reassigned to different carrier services on a call-by-call basis [Ref. 29:p. 49]. While the United States, Canada, and Japan have a standardized on a PRI of 1.544 Mbps, Europe's standardized rate is 2.048 Mbps. The European channel structure consist of 30 B-channels plus one 64 kbps D-channel. Although only the B- and D-channels permeate GOSIP documents, there are several other access channels defined by ISDN: A-, C-, E- and H-channels. Three of these channels are further examined below: B-, D-, and the H-channels.

c. Access Channels

1. B-Channel

The B-channel is used for transparent exchange of user data. This channel can be used to carry digital data, PCM-encoded digital voice, or a mixture of lower-rate traffic, including digital data and digitized voice encoded at a fraction of 64 kbps. Although 64 kbps rate was chosen as the most effective rate for digitized voice, technology has progressed to the point where 32, 16 or even 8 kbps will produce equally satisfactory voice reproduction. When multimedia applications are used over the B-channel, all traffic on the channel must be destined for the same endpoint; that is, the elementary unit of circuit switching is the B-channel. If a B-channel consists of two or more subchannels, all subchannels must be carried over the same circuit between the same subscribers. The B-channel can be used for circuit-switching, semipermanent circuits, and packet-switching. The circuit-switch connection is equivalent to the switched digital service offered today. The call setup is not done over the B-channel but over the D-channel instead. The semipermanent connection, also called a dedicated circuit, is a pre-established connection between users and does not require a call request protocol. The packet-switched connections interface to a packet-switch node (PSN) where data is exchanged using X.25. FIPS 146-1 list six ways in which an ISDN B-channel can be used by a GOSIP end system [Ref. 22-1:p. 15]:

- circuit-switched access to a packet handler integral to an ISDN switch;
- circuit-switched access to a packet handler separate from an ISDN switch;

- circuit-switched access directly to another GOSIP end system, or GOSIP intermediate system;
- dedicated circuit access to a packet handler integral to an ISDN switch;
- dedicated circuit access to a packet handler separate from an ISDN switch, and
- dedicated circuit access to another GOSIP end system or GOSIP intermediate system.

2. D-Channel

The D-channel is used to exchange control information between the user and the network for call establishment, maintenance, and termination. The D-channel is a logical channel which serves two main purposes. First, it carries common channel signalling information to control circuit-switch calls on associated B-channels at the user interface. The user's request is sent over the D-channel uninhibited by overhead. The second purpose of the D-channel is that it may be used for packet-switching or for low-speed user data (e.g., 100 bps) when no signalling information is waiting. The maximum data rates for on the D-channel for BRI is 16 kbps and for PRI its 64 kbps. A new data link layer standard called LAP-D has been defined for the D-channel. All transmission on this channel is in the form of LAP-D frames, exchanged between the subscriber equipment and an ISDN switching element (LAP-D is detailed later in this section). When packet-switched connection is desired the X.25 packet layer protocol is used to establish virtual circuits over the D-channel to other users, and to exchange packetized data. One of the key differences between this and the B-channel is that this channel is always present; hence no layer 3 call control is required. The user's request is done at layer 2 over the D-channel [Ref. 28:p. 30]. In short, the D-channel

supports three type applications [Ref. 25:p. 277]: control signalling, packet-switching, and telemetry. There is no contention or potential degradation because the D-channel is basically clear.

3. H-Channels

Narrowband ISDN supports the H-channel as non-switched or circuit-switched service at the PRI. These channels are designated as H_0, H_{11}, and H_{12} and set to operate at 384, 1536, or 1920 kbps, respectively. They must rely on a 64 kbps D-channel for control signalling. When no D-channel is present on the interface, it assumes that a D-channel on another PRI at the same subscriber location will provide any required signalling. The following combinatorial structures are possible over the H-channel using the primary rate interface [Ref. 25:p. 246]:

- H_0 channel structures: This interface supports multiple 384-kbps H_0 channels. The structures are $3H_0 + D$ and $4H_0$ for the 1.544-Mbps interface and $H_0 + D$ for the 2.048-Mbps interface.

- H_1 channel structures: The H_{11} channel structure consists of one 1536-kbps H_{11} channel. The H_{12} channel structure consists of one 1920-kbps H_{12} channel and one D-channel.

- Mixtures of B and H_0 channels: Consist of zero or one D-channels plus any possible combination of B and H_0 channels up to the capacity of the physical interface (e.g. $3H_0 + B + D$ and $3H_0 + 6B$).

The H-channel provides user information at higher bit rates grouped at high bandwidth. The channel can be used as a high-speed trunk or subdivided according to the user's own time-division multiplexing (TDM) scheme. Many ISDN vendors offer the H-channel as part of their ISDN services. Table IV-2 represents some of the

potential applications available on the H-channels as well as the B- and D-channels [Ref. 25:p. 245]. The use of the H-channels for B-ISDN is discussed in Chapter V.

TABLE IV-2
ISDN CHANNEL FUNCTIONS/APPLICATIONS

B-Channel (64 kbps)	D-Channel (16 kbps)	H-Channel (384, 1536, 1920 kbps)
Digital Voice 64 kbps PCM	Signalling Basic Enhanced	Multiplexed Info Streams
High-Speed Data Circuit-Switched Packet-Switched	Low-speed data Videotext Terminal	High-Speed Data Video
Other Facsimile Slow-Scan Video	Telemetry Emergency Service Energy Management	Fast Facsimile High-Quality Audio

3. Data Link Layer and Services

Data link ensure reliable transfer of data across the physical layer. Several of the link standards associated with this level are HDLC, LLC, LAP-B, and LAP-D. GOSIP specifies HDLC and LAP-B for use in conjunction with X.25 and point-to-point networks. FIPS-146-1 specifies the use of Q.921 (LAP-D) for operation on the ISDN D-channel [Ref. 21:p. 13].

a. Link Access Protocol-D (LAP-D)

LAP-D is a layer 2 standard developed as part of the ISDN standardization effort. It is addressed in the I-series Recommendation I.440 and I.441. The "D" designation signifies that this a D-channel service. LAP-D is modeled after the

LAP-B protocol used in X.25 and on HDLC. The purpose of LAP-D is to convey information between layer 3 entities across the ISDN user-network interface. It specifies a link access protocol that is part of a time-multiplexed link between network subscriber and the ISDN central office. LAP-D is independent of transmission bit rate and requires a duplex, bit transparent D-channel [Ref. 25:p. 292]. All traffics on this circuit (both user and protocol control information and parameters) are carried using LAP-D frames which provide two forms of service to the user: the unacknowledged information transfer service and the acknowledged information transfer service. Both of these services may coexist on the D-channel [Ref. 18:p. 732]. The unacknowledged information transfer service provides for the transfer of user data (frames) without acknowledgement. It does not guarantee deliver, nor does it inform the sender of failed delivery. The acknowledge information transfer service is more common and similar to the services of LAP-B and HDLC. With this service, a logical connection is established between two LAP-D users prior to exchanging data which is used for connection establishment, data transfer, and connection termination. This logical LAP-D connection guarantees that all frames will be delivered in the order they were transmitted. Figure 20 represents the structure of a LAP-D frame [Ref 25:p. 293].

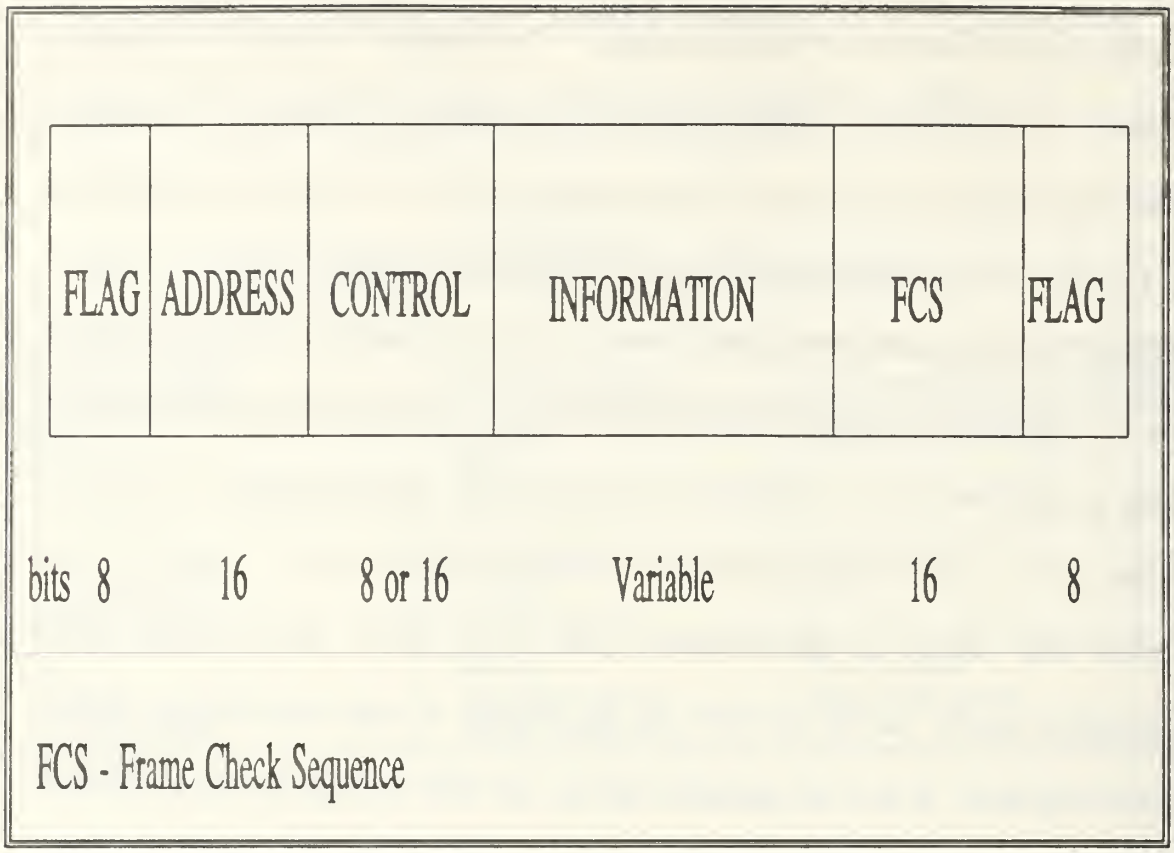


Figure 20
LAP-D Frame Format

b. LAP-D Addressing

In the LAP-D framing structure, a 2-octet field is used to address end points: a terminal endpoint identifier (TEI) and a service access point identifier (SAPI). Figure 21 shows the octet assignments of these two identifiers [Ref. 25:p. 294]. The first octet carries a TEI and the second octet carries a SAPI. TEI is used for multipoint operations. Usually, each user device is given a unique TEI but it is also possible for a single device to be assigned more than one (e.g., a terminal concentrator). Assignments of TEIs can be performed either automatically (when the equipment is first

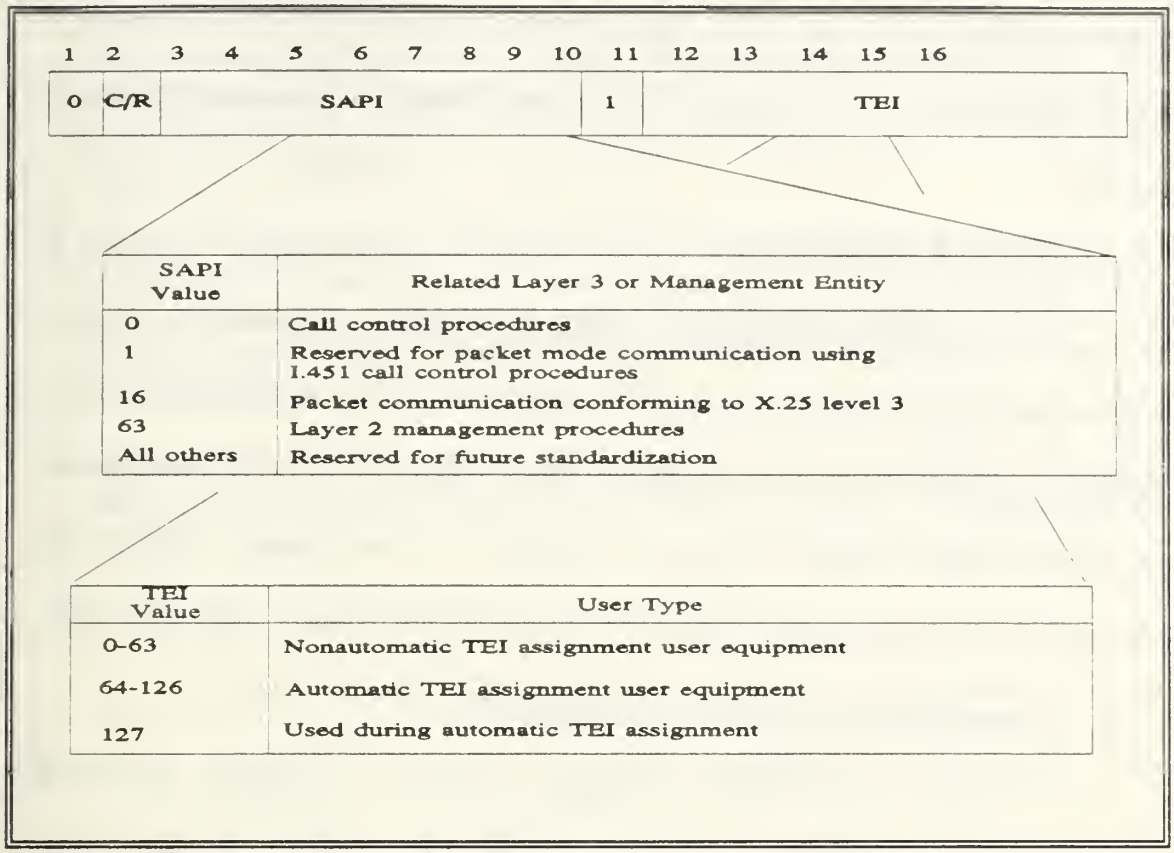


Figure 21
TEI and SAPI Address Field Format

connected to the network), or manually. Automatic assignment of the TEI allows the user to freely change, add, or delete equipment without prior notification of the network administrator. However, caution must be taken with the manual assignment of TEIs, since it is possible for multiple equipment attached to the same interface to have identical TEIs. The SAPI permits separate, independent frame windows for each separate function (e.g., call control versus packet traffic) [Ref. 28:p. 29]. Each SAPI value is unique within a TEI. The SAPI identifies a layer 3 user and distinguishes between the various traffic types [Ref. 22:p. 97]. The address field of the LAP-D frame format also includes

a command/respond (C/R) bit which is used to communicate the type of message contained in the frame. This can either be a command message or a message demanding a response.

c. LAP-D Windowing

A window represents a number of frames or packets that may be outstanding at one time. While X.25 LAP-B allows both 3- and 7-bit windowing, there were never any commercial HDLC chips that fully support the larger 7-bit windows. With a 3-bit window means that up to 7 frames can be outstanding. Thus, 7-bit windowing was chosen because it allows for 127 outstanding frames. [Ref. 28:p. 29]

4. Network Layer and Services (Q.931/I.451)

The ISDN User-Network Interface (layer 3) is defined in CCITT Recommendation Q.931-1988 (also designated CCITT Recommendation I.451-1988) [Ref. 30:p. 4-7]. Q.931 (call control) is used for access signalling, when appropriate, to select the B- or D-channel for packet data transfer and for establishing and releasing a physical path on ISDN [Ref. 31:p. 12]. The protocol at this layer only exists at the network-to-user interface on the D-channel to perform users request for services [Ref 25:p. 306]. In the packet mode, there are a number of major configuration scenarios possible. Several major packet mode scenarios are described below:

- Circuit-switch access to a packet-switched Public Data Network (PSPDN). In this case, the ISDN to which the user is attached (locally) provides circuit-switched service for the call. The local network is not aware that this is a packet call. This type service is mostly used when the local network does not provide packet-switched service. Once the circuit-switch access is established, multiple virtual circuits may share the access connection.

- B-Channel packet access. This service is provided by the local network. To the user, it appears that the local switch is providing the packet-switched services. The user must set up a packet-switch call to allocate a B-channel. Like in the circuit-switch scenario above, once the connection is established, multiple virtual circuits may share the connection.

- D-Channel packet access. As in the previous case, this service is provided by the local ISDN. The key difference from the previous case is that the D-channel is always present. Consequently, no layer 3 call control is required. The user can start with a layer 2 packet communication conforming to X.25 layer 3 (SAPI=16) on the D-channel.

- Permanent access circuits. These unswitched circuits does not require call control. They can be used with either the local service provider or a remote service provider.

CCITT has defined 30 or more I.451 messages associated with circuit-switched call control [Ref. 25:p. 306]. Stallings identifies two basic types of user devices supported: functional and stimulus. Functional terminals are intelligent devices and can employ the full range of I.451 messages and parameters for call control (e.g. ISDN terminal). The other device (stimulus terminal) could be a simple telephone. I.451 messages are sent to the network by a stimulus; activated by simply removing the telephone handset or depressing a key.

5. Signalling System Number 7 (SS7)

One of the significant enhancements in integrated digital networking and control is the advent of SS7. SS7 is the mechanism that provides the internal control and specifically designed to be used in ISDN. It provides the network intelligence essential to ISDN. One of the unique features of SS7 is its fast and virtually unlimited signalling

capability while the communication is being established [Ref. 32:p. 102]. It offers a more flexible and efficient means of control signalling than in-band signalling schemes such as multi-frequency and robbed-bit. Unlike other schemes, SS7 covers all aspects of control signalling for complex digital networks; including the reliable routing and delivery of control messages and the application-oriented content of those messages. Stallings lists five primary characteristics of SS7 [Ref. 25:p. 122]:

- It is optimized for use in digital telecommunications networks in conjunction with digital stored program control exchanges utilizing 64-kbps digital channels.
- It is designed to meet present and future information transfer requirements for call control, remote network management, and maintenance.
- It provides a reliable means for the transfer of information in the correct sequence without loss or duplication.
- It is suitable for operating over analog channels and at speeds below 64 kbps.
- It is suitable for use on point-to-point terrestrial and satellite links

At the network-to-network level (between switches), SS7 is used and may take a completely different route for traffic than the user's data [Ref. 25:p. 306].

a. SS7 Architecture

The term architecture, as related to SS7, is used to describe a relationship with the OSI Reference Model. Figure 22 shows this relationship [Ref. 18:p. 738]. The SS7 architecture consists of four levels. Layers 1 through 3 are the signalling data link, the signalling link, and the signalling network, respectively. These three layers are referred to as the Message Transfer Part (MTP). At the fourth layer is the signalling

connection control part (SCCP) module. Collectively, the MTP and the SCCP are called the Network Service Part (NSP). Also the fourth layer of the SS7 architecture includes the ISDN User Part (ISUP), the Telephone User Part (TUP) and the Transaction Capabilities Application Part (TCAP). The TCAP provides the mechanisms for transaction-oriented (as opposed to connection-oriented) applications and functions. Each of these components, except the TCAP, are discussed in further detail below.

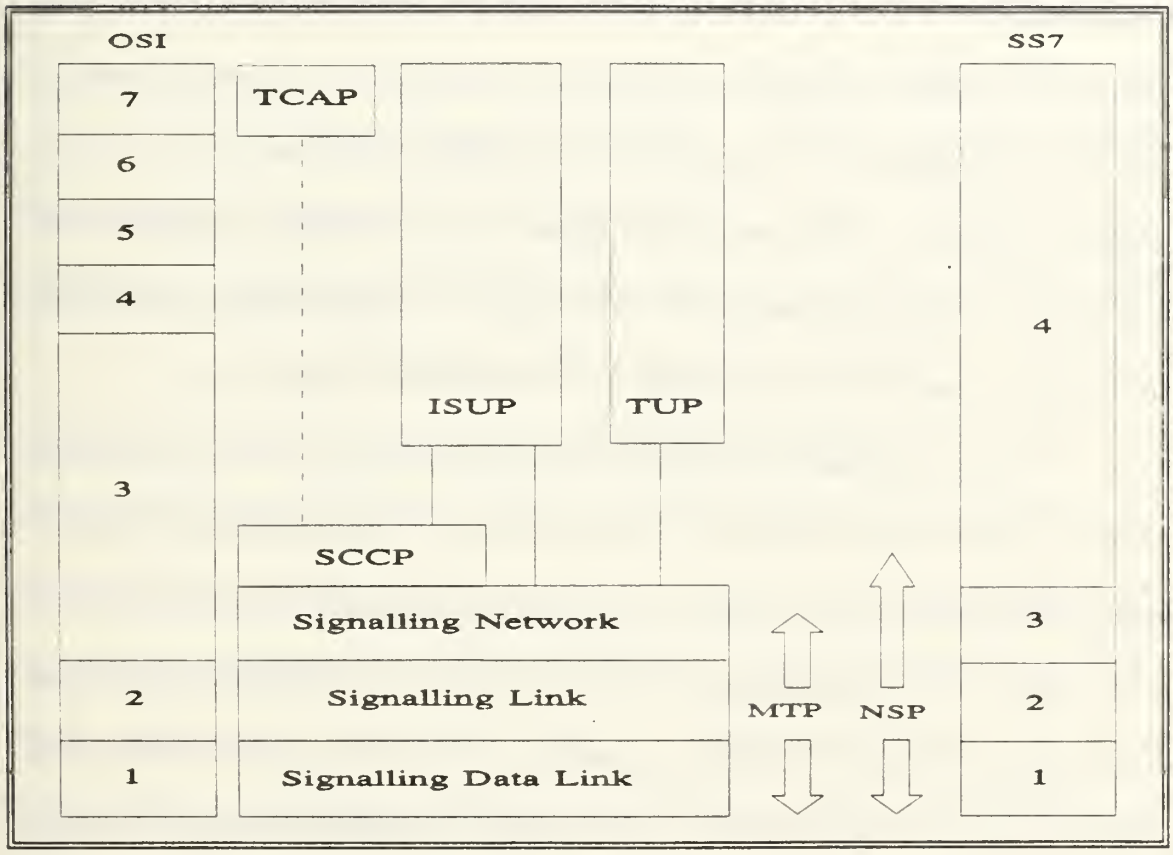


Figure 22
SS7 Protocol Architecture

(1) Message Transfer Part (MTP). The MTP is described in CCITT (1988) Recommendations Q.701-Q.710. It provides a reliable but connectionless (datagram type) service for routing messages through the SS7 network. MTP service is similar to that of X.25 for packet-switched networks. Three elements comprise the MTP: (1) signalling data link, (2) signalling link and, (3) the signalling network functions. The signalling data link is the lowest level of the SS7 architecture and is concerned with the physical and electrical characteristics of the signalling links. The signalling link level is a control protocol that provides for the reliable sequenced delivery of data across a signalling data link. The top level of the MTP is the signalling network. It provides for routing data across multiple control points from control source to control destination. However, these three levels together do not provide the complete set of functions and services specified in the OSI layers 1-3, most notably in the areas addressing and connection-oriented service (i.e., CONS) [Ref. 18:p. 737].

(2) Signalling Connection Control Part (SCCP). Q.71X series details the SCCP. The SCCP provides the full OSI Network Layer functions not included in the original message transfer part, such as full global addressing and connection control. It can be used for end-to-end signalling whether or not there is a circuit established between the message originating and terminating exchanges. Here the msg route is determined by SCCP and may not relate to any user. For example, the message distribution function provides only a limited addressing capability. For newer user part applications, a more complex specification of a message at a node is necessary. The SCCP enhances the connectionless sequenced transmission service provided by the MTP, to meet the needs

of those user parts requiring enriched connectionless or connection-oriented service. For those user parts for which MTP suffices, the extra overhead of SCCP can be avoided. There are five classes of network service defined for SCCP [Ref. 25:p. 138][11]:

- 0 - Basic unsequenced connectionless
- 1 - Sequenced (fixed signalling link selection number) connectionless class
- 2 - Basic connection-oriented
- 3 - flow control connection-oriented
- 4 - error recovery and flow control connection-oriented

(3) Network Service Part (NSP). The NSP is simply a message delivery system. It consists of the SCCP and the MTP. A variety of different network-layer services are defined in the SCCP to meet the needs of various users of the NSP.

(4) ISDN User Part (ISUP). Details of the ISUP are addressed in Q.76X of CCITT (1988) recommendations. ISUP defines the functions, procedures, and interexchange signalling information flows required to provide circuit-switched services and associated user facilities for voice and non-voice calls over ISDN. The ISUP utilizes the transport capabilities of the MTP and SCCP to provide call-related services for ISDN. Because of the overall role of SS7 in providing interexchange signalling for ISDN, there is a correspondence between many of the capabilities of the ISUP and the I.45x series of control signal specifications. Stallings states three requirements for the

[11]Only classes 0 and 1 have been fully specified.

ISUP [Ref. 25:p. 314]: (1) it must rely on the message transfer part or network service part of SS7 for the transmission of messages, (2) its design must be flexible to accommodate future enhancements of ISDN capabilities, and (3) it must interwork with the user-network I.451 call control protocol. This last item is very important in discerning Q.761-Q.766 and I.451. The call control protocol defined in I.451 refers to common channel control signalling facilities open for use by the ISDN subscriber. I.451 is used by the subscriber with associated user facilities. ISUP refers to signalling facilities employed by the network provider on behalf of the ISDN user. Thus, ISDN communicates with the ISDN subscriber via I.451 for the purpose of call control, and uses ISUP internal to the network to implement subscriber call control requests. The term "user part" does not refer to the ISDN user; rather, it refers to the fact that the ISUP is a user of the lower layers of SS7.

(5) Telephone User Part (TUP). The TUP is addressed in Q.72X. It utilizes the transport capabilities of the MTP to provide circuit-related signalling for telephone call control over both digital and analog circuits. TUP is invoked in response to actions by a subscriber at a telephone. For example, when a handset is lifted from its cradle, it sends signals through the network requesting a circuit. As a whole, TUP control signals accomplish the establishment, maintenance, and termination of telephone calls.

b. SS7 Configuration

There are three circuit components supporting SS7: Service Control Points (SCPs), Signal Transfer Points (STPs), and Service Switching Points (SSPs).

SCP, the most important, is the real intelligence of an SS7 network. It comprises a collection of database computers that provides a central network resource for customer and routing information in connection with network services. The STPs are regional switches which allows routing and service parameters to be aggregated at the tandem switch level. [Ref. 33:p. 16] The SSP are software packages for local exchange or tandem switches that adapt the switch for interaction with SCPs over an SS7 network. Collectively, these circuit components communicate between other switches to form the SS7 network. This could be for enterprise-wide or autonomous connections and services. Figure 23 provides an illustration of how SS7 overlays a packet-switch network.

c. SS7 Comparison to X.25

Both SS7 and X.25 deal with packet-switch networks. However, their applications are very different in function, protocol structure, modes of operation, block formats, etc. For example, X.25 defines an interface between a subscriber device and a packet-switched network. It contains both control signalling (call setup and termination) and subscriber data transfer functions. SS7 is primarily for the use of applications residing in the combined circuit-switched/packet-switched network, although the ISDN user part relates to subscriber devices. It contains only control signal information and is concerned with the internal structure of the network (i.e., routing, reliability, and performance) [Ref. 22:p. 15]. Table IV-3 on page 97 shows a comparison of other major features of CCITT X.25 and CCITT SS7 [Ref. 25:p. 139].

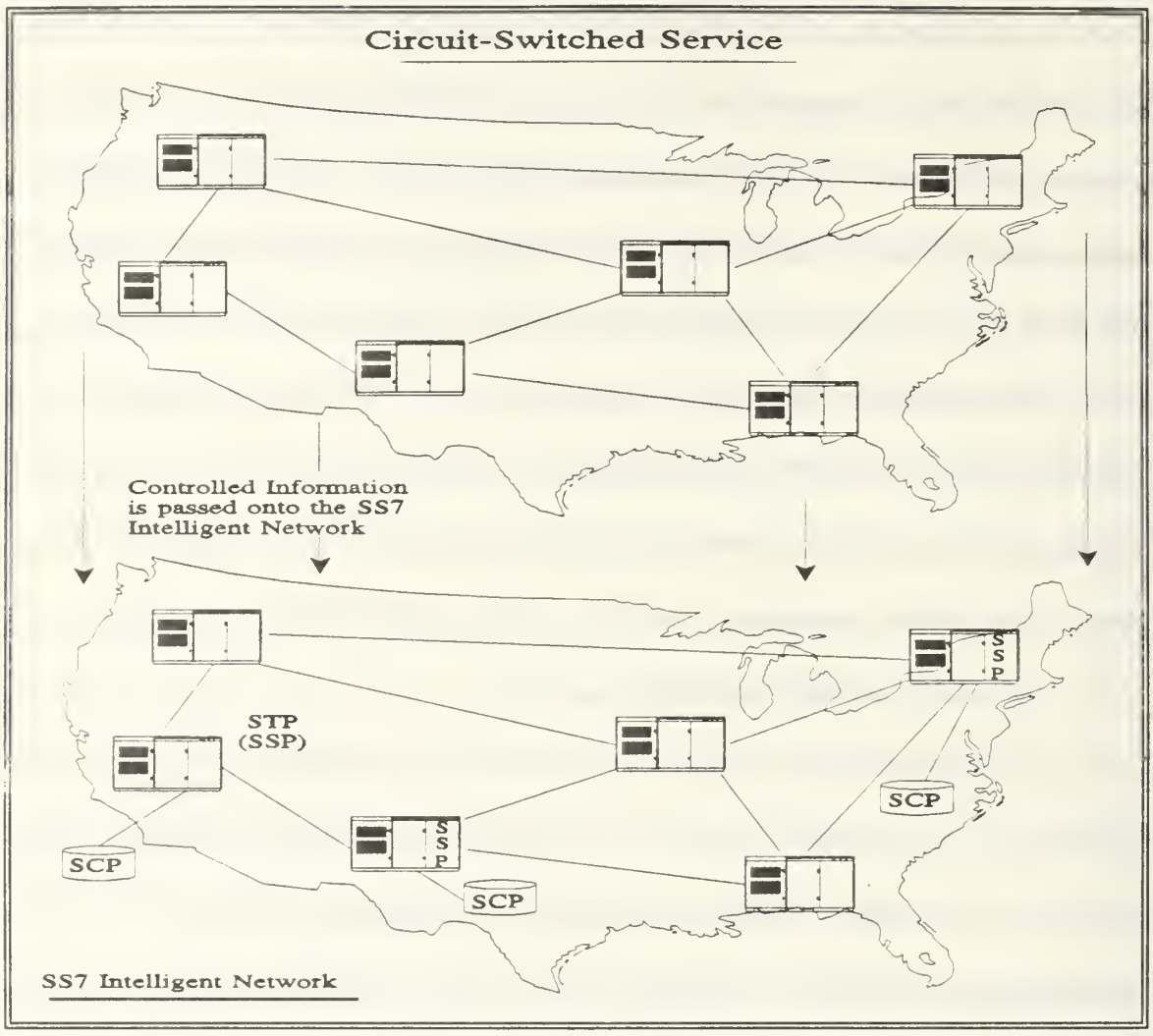


Figure 23
Conceptual View of SS7 Network

TABLE IV-3
COMPARISON OF X.25 AND CCITT SS7

Description	CCITT X.25	CCITT SS7	Comments
Function	Procedure for connecting data equipment to packet network	Procedure for CCS. Includes: call control, mgt, and maintenance signalling	
Functional Division	One: Data Communications	Two: (1) MTP and (2) Specific User Parts	MTP specifies data comm function and its performance
Protocol Structure	Three Levels	Four Levels	The lower three layers are equivalent
Modes of Operation	SVC or Autoconnect	Preestablished path equivalent to X.25 Autoconnect	
Level I	2.4 to 56 kbps	Optimized for 64 kbps down to 4.8 kbps	
Level II	HDLC	SS7 Level 2	
Outstanding Blocks	8	128	
Address Field	8 bits	Not Required	
Error Control	CRC	CRC	
Routing	By packet header	By routing label	

The number of ISDN offerings are increasing although the standards are still being developed. This has, unfortunately, presented interoperability problems at both the user-to-network level and the network-to-network (signalling) level. For example, Northern Telecom's DMS-100 BRI channel is incompatible with AT&T's 5ESS, Siemems Information EWSD switch or Ericsson's AXE switch [Ref. 29:p. 50]. Similarly, SS7 implementations by Pacific Bell, Southwestern Bell, and Ameritech and

ANSI standards. However, offerings from NYNEX, US West, and Bell South implementations are based only on CCITT [Ref. 34:p. 25].

D. DoD ISDN PROFILES

The primary sources for ISDN standards within the DoD are the Stable Implementation Agreements for Integrated Services Network (developed by the ISDN Implementor's Workshop of the NIU-Forum) and the Stable Implementation Agreements for Open Systems Interconnection Protocols (developed by the OSI Implementors' Workshop). These documents contain implementation specifications that are derived from services and protocol standards issued by CCITT and ANSI [Ref. 28:p. 1]. Within the military, the primary source for the ISDN Profiles are addressed in MIL-STD 188-194, Integrated Services Digital Network Profiles (ISDNP). The DoD ISDN profiles are based on standards developed by CCITT, ANSI, and agreements reached by the ISDN Implementors' Workshop under the auspices of the NIU-Forum. This military standard defines a common set of specifications to facilitate interoperation among products and services capable of interoperating across activity, service, and agency boundaries without regard to proprietary limitations.

1. Mandatory Profiles

The following list highlights the mandatory bearer services for all departments and agencies of the DoD [Ref. 28:p. 14]. This includes both for PBXs and switches:

- circuit-mode digital (CMD)
- circuit-mode voice (CV)

- circuit-mode voiceband data (CVBD)
- circuit-switched access to a packet-switching node
- B-channel packet-switched access
- D-channel packet-switched access on the basic rate interface

2. Optional Profiles

The optional services specified for use within DoD are [Ref. 28:p. 14]:

- Multi-rate bearer service
- H_0 - 384 kbps
- H_{10} - 1472 kbps
- H_{11} - 1536 kbps
- 7-kHz Multi-use service
- Frame relay service (T1.606)
- User signalling bearer service (T1S1/LB91-01)

The transmission structure of the H-channel, defined under ISDN, differs slightly from the structure of the DoD optional profiles. CCITT is standardized at rates of 384, 1536, or 1920 kbps. The optional H-channel service specified by the DoD are at rates of 384, 1472, and 1536 kbps and are identified as H_0, H_{10}, and H_{11}, respectively. Use of this channel could potentially provide equal or faster data rates than that of the B-channel. Additionally, it could reduce some of the overhead resources and network management associated with channel maintenance. The MILDEPs will encounter

incompatibility between ISDN switches by the various vendors. It is expected that other ISDN vendors products will likewise, have similar incompatibility problems.

E. PROPOSED ISDN FEDERAL INFORMATION PROCESSING STANDARD (FIPS)

Federal Information Processing Standards (FIPS) establishes standards and guidelines for use by federal agencies. A FIPS for ISDN is being developed to be compatible with FIPS 146-1 (GOSIP). The proposed standard defines the generic protocols necessary to establish transparent ISDN connections among and between government networks and conformant common carrier networks. It provides a minimal set of bearer services, and is based on national standards, international standards, and implementation agreements developed by the NIU-Forum. The Federal Register describes the primary objective of the new ISDN information standard [Ref. 27:p. 1256]:

- To achieve interconnection and interoperability of user and network equipment that are acquired from different manufacturers in an open systems environment;
- To reduce the cost of acquiring user equipment for ISDN services;
- To facilitate the use of advanced technology by the Federal Government;
- To stimulate the development of commercial products compatible with ISDN standards.

Besides those mentioned above, the new FIPS will also address protocols and implementation agreements for the D-channel procedures at layers 1, 2, and 3 for ISDN protocols as well as a limited set of other protocols, such as ISDN bearer services, X.25

Packet Services, and Terminal Adaptation [Ref. 27:p. 1257]. SS7 protocols are not included. NIST plans to issue a variety of FIPS to exploit the full technical capabilities of ISDN. The initial focus aims at switched 64 kbps service for voice and voice/data; and in GOSIP, it will address OSI data using both the basic and primary rates.

F. NATIONAL INTEGRATED SERVICES DIGITAL NETWORK (NATIONAL ISDN)

Perhaps the most significant recent activity in the area of ISDN is the evolution of National ISDN-1. One of the major goals of National ISDN-1 is to bring narrowband ISDN capability to large groups of users throughout the U.S. [Ref. 35:p. 20]. National ISDN-1 gives customers the ability to operate in a multi-vendor ISDN environment by providing interswitch/internetwork connectivity, access to pre-ISDN analog and digital services, uniform protocol interfaces at layers 1, 2, and 3, (protocol portability), and interworking with pre-National ISDN-1 ISDN users [Ref. 36:p. 7-1]. Vendors that have joined in this commitment to National ISDN-1 include AT&T, Northern Telecom, Siemens Stromberg-Carlson, Apple, Bell Atlantic, Bell Corporation Research (Bellcore), Boeing, Digital Equipment Corporation, General Motors, IBM, Kodak, Motorola, NYNEX, and Southwestern Bell [Ref. 35:p. 20]. Much of the groundwork has been laid for nationwide implementation and is expected to make its formal debut in late 1992. Adoption of National ISDN-1 is the first significant step toward a full interoperable multi-vendor network foundation for ISDN in the U.S. For users, National ISDN-1 will

mean immediate capabilities for digital networking available ubiquitously throughout the United States.

G. SUMMARY

ISDN is expected to be deployed on a wide scale in ubiquitous public offerings and in private network offerings, as services and as components from which private ISDN networks can be constructed. Initial offerings will be a switched 64 kbps service delivered to a customer's terminal at a basic rate (16 kbps signalling channel and two 64-kbps data channels) or a primary rate (24 64-kbps channels, one used for signalling) [Ref. 21:p. 61]. GOSIP Version 2 incorporates ISDN as the latest subnetwork technology for use by federal and DoD agencies. The two ISDN access channels addressed by GOSIP may offer substantial benefits for the government in terms of cost, flexibility, security and privacy, and integration of heterogeneous "islands" of networked systems. While the demand for increased services continues, the deployment of ISDN on a full-scale basis has yet to be realized. The efforts by NIST, in cooperation with the NIU-Forum, is attempting to accelerate this technology through implementation of National ISDN-1. The military services will no doubt be hindered by the slow development of the ISDN services. It will be extremely advantageous if attempts be made to influence the standards to meet service unique requirements and to ensure that ISDN will be deployed throughout the military with minimal impact to existing plain old telephone systems (POTS). The planning for ISDN began as far back as 1976.

Although the full spectrum has yet to be realized, planning and the development of a new network concept is occurring. This new concept is called Broadband ISDN.

V. OVERVIEW OF BROADBAND ISDN (B-ISDN) AND OTHER DIGITAL TECHNOLOGIES

A. BROADBAND-ISDN

1. Background, Concept and Objective

The primary motivation toward B-ISDN is the increased demand for high bit rate services; especially image and video services. B-ISDN is a fast packet-based network designed to provide increased bandwidth (by orders of magnitude) beyond that of conventional ISDN. It is envisioned as an all-purpose, wide-area digital network, intended to meet the growing demand for broadband services such as video-based communications; using the same switching and transmission vehicle. There are two major improvements of B-ISDN over conventional ISDN; they include the use of optical fiber and Fast Packet Switching (FPS) technology based on the Asynchronous Transmission Mode (ATM). Fiber optics is the technology available today to meet user high-resolution video requirements and the multi-channel rate of the network to handle these multiple video users. FPS is a "streamlined" packet switching technology and includes two evolving principles: cell relay and frame relay. Cell relay (in terms of ATM) will be discussed in the following section and frame relay is detailed is Section B. FPS provides the benefit of reduced protocol processing (i.e., high throughput and low delay) while retaining the advantage of packet switching (i.e., efficient use of transmission facilities). Streamlining is designed to overcome some of the weakness of

traditional packet switching such as large and variable delays. The key aspect of streamlining include:

- Elimination of "link-by-link" error and flow control. The high quality and speed of modern digital transmission trunks, such as optical fiber links, eliminate the need for error and flow control on a per-link basis.

- Elimination of network layer processing. Permanent virtual circuits (PVCs) are set up administratively via the network management system to provide fixed routing rather than on a call-by-call basis.

Like ISDN, B-ISDN offers the use of H-channel rates but at much higher. CCITT has produced a preliminary definition of these new channel rates to be added to the existing narrowband channel rates. These rates are reflected in Table V-1 on the following page [Ref. 25:p. 350]. Note that the capacity of the H-channels exceeds the channel rates offered by narrowband ISDN. The recommendation specifies that the H_2 and the H_4 rates be in multiples of 64 kbps. Both the H_{21} and H_{22} rates can support full-motion video for conferencing (without compression), video telephone, and video messaging while the H_4 rate is designed for bulk data transfer of text, facsimile, and enhanced video information.

TABLE V-1
NARROWBAND AND PROPOSED BROADBAND CHANNELS

Channel	Data Rate	Applications
		Narrowband ISDN
D	16 or 64 kbps	control signalling; packet-switched data circuit- and packet-switched data, voice, facsimile, compressed video
B	64 kbps	
H_0	384 kbps	PBX access, compressed video, high-speed data
H_{11}	1.36 Mbps	PBX access, compressed video, high-speed data
H_{12}	1.920 Mbps	
		Broadband ISDN
H_2 (H_{21} and H_{22})	30-45 Mbps	Full-motion video for conferencing, video telephone, or video messaging
H_3	60-70 Mbps	Not identified
H_4	120-140- Mbps	Bulk data transfer of text, facsimile, enhanced video information

2. Asynchronous Transfer Mode (ATM) and Characteristics

ATM is a next generation cell-switching technology that packages data in 53-byte fixed cells for high-speed transmission. The 53-byte cell is composed of a 5-byte header and a 48-byte data. Because this is fixed cell, it provides uniform delay which is ideally suited to support voice/video transmission in isochronous channels. All ATM cells are dynamically assigned on demand. ATM is, in essence, a form of packet transmission across the user-network interface in the same way that X.25 is a form of

packet transmission across the user-network interface. One difference between X.25 and ATM is that X.25 includes control signalling on the same channel as data transfer, whereas, with ATM, user information and control signalling are carried on separate virtual channels. The use of ATM creates the need for an adaption layer to support information transfer protocols not based on ATM. Figure 24 illustrates an architectural model of the B-ISDN protocol for ATM [Ref. 18:p. 747]. Two examples using an

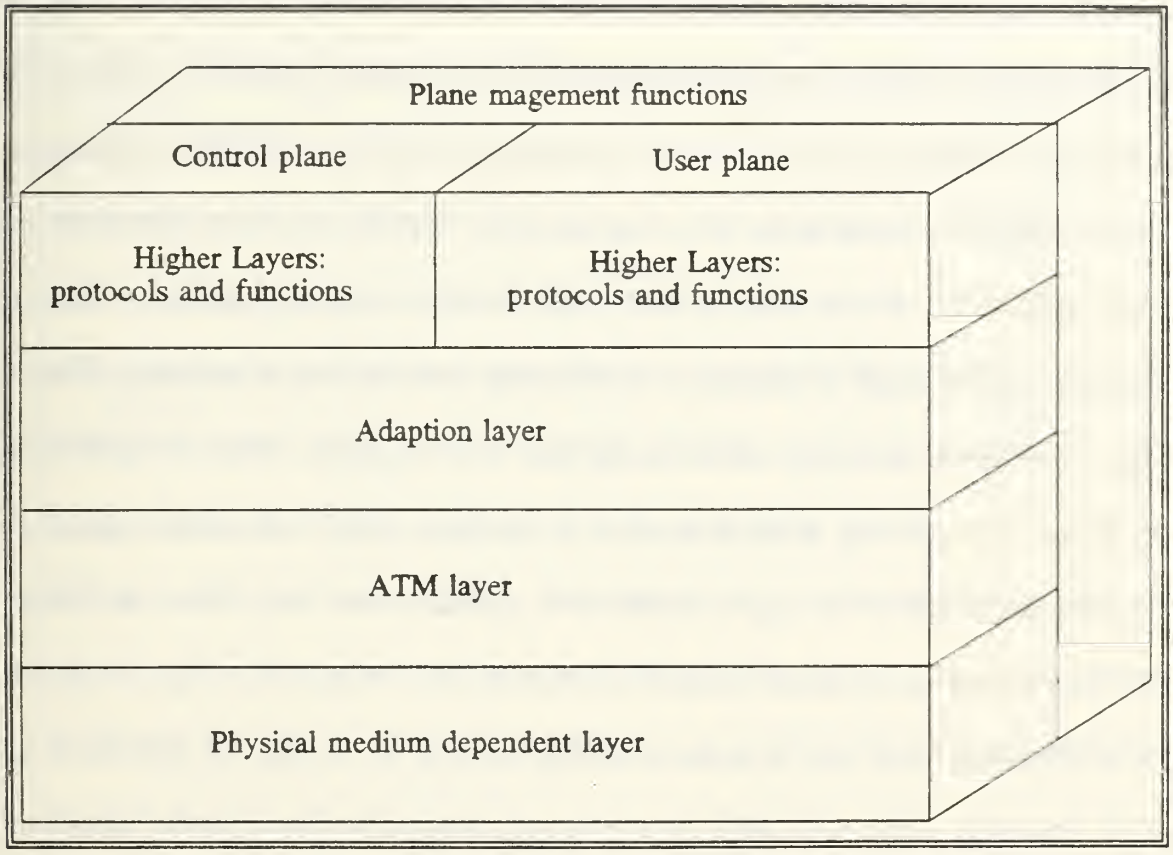


Figure 24
B-ISDN Protocol Model for ATM

adaption layer are: (1) pulse code modulation (PCM) voice and (2) LAP-D. PCM voice is an application that produces a stream of bits. To employ this application over ATM,

it is necessary to assemble PCM bits into packets or cells for transmission and to read them out upon receipt in such a way to produce a smooth, constant flow of bits to the receiver. For LAP-D, it is necessary to map LAP-D frames into ATM packets; essentially segmenting one LAP-D frame into a number of packets on transmission, and reassembling the frame from packets on reception. By allowing the use of LAP-D over ATM, all of the existing ISDN applications and control signalling protocols can be used on B-ISDN. ATM is the target solution for the B-ISDN user-network interface. This implies that B-ISDN will be a packet-based network at the interface and perhaps in terms of its internal switching. The two bit rates proposed by CCITT for B-ISDN subscribers (150 and 600 Mbps) is based on the following rationale. The data rate from network to user will need to be on the order of 600 Mbps in order to handle multiple video distributions, such as might be required in an office environment or even at home. The data rate from user to network would normally need to be much less, hence the smaller rate is used. The evolving B-ISDN standard at this layer (CCITT Recommendation I.121) states that B-ISDN will support circuit-mode applications as well. However, this will be done over a packet-based transport mechanism [Ref. 18:p. 747]. This permits ISDN to transform itself into a packet-switching network as it takes on broadband services. The local exchange to which subscribers attach must be able to handle both B-ISDN and ISDN subscribers.

3. Current Direction of B-ISDN

Some in industry envisions a complex, multi-featured broadband network by 1994. However, Walters, in his article, believes that this may be too aggressive and that public switched networks will not be technologically capable to make a flash-cut by this time. His belief is predicated on two issues [Ref. 37:p. 36]: (1) a lack of B-ISDN defined capabilities and (2) the preliminary transport and switching systems requirements. B-ISDN capabilities are still under development, although some standards committees like, CCITT, T1 and ETSI are actively working to define the capability. Secondly, preliminary transport and switching services, using these services over SONET/ATM, are based on extensions to ISDNs Q.931 protocol. User requirements will include such services as transmitting large multimedia files containing photographic quality images and video snippets, and to perform desktop multimedia teleconferencing including video and, later, high-resolution video. These services demand high-speed transmission and switching within the interconnection network, and many require new signalling capabilities well beyond that of Q.931. For example, in a asymmetrical connection for transport, requires renegotiation of the basic attributes of the various connections making up a call and the addition of new connections to an existing call when an additional median is invoked and adding new legs to a call [Ref. 37:p. 39]. Many of these capabilities are made even more complex when additional services are considered, e.g., three-way calling, closed user groups, call forwarding, and voice mail. These services are important, especially to users of new multimedia videotelephony workstations who desire to use it in lieu of a telephone.

4. Future Direction of B-ISDN

Figure 25 conceptualizes a B-ISDN architecture [Ref. 37:p. 39]. There is little doubt that multimedia applications is probably the largest, single most user requirement driving the implementation of B-ISDN. Many vendors are developing B-ISDN switching products (e.g., multimedia bridges) to keep pace with B-ISDN development while supporting existing users applications. For example, future

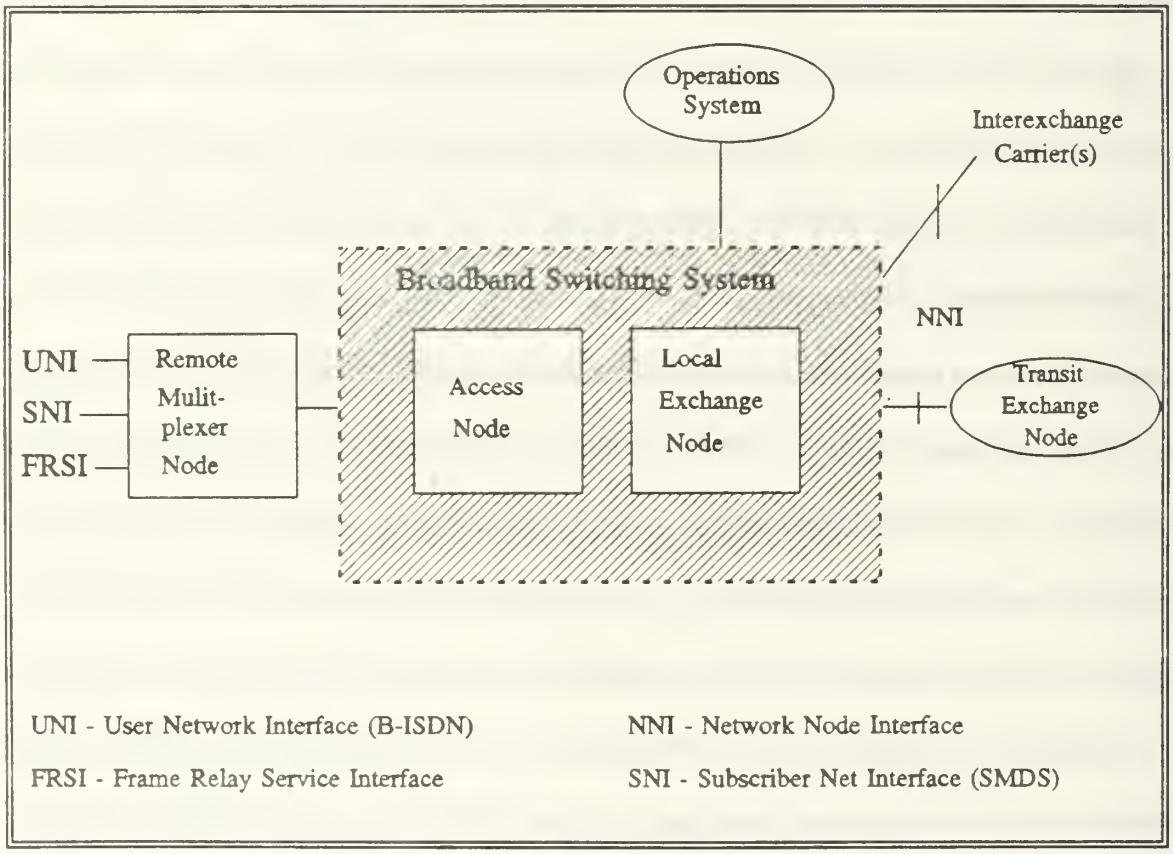


Figure 25
B-ISDN Architecture

development of multimedia bridges for conferencing parties should be based on H.261 video, μ/A-law coded audio, graphics, images, and other media [Ref. 37:p. 42]. It may

be possible through the addition of processors and software to ease the stigma of migration problems normally associated with new technological paths. One of the major impacts that B-ISDN will have on the C^3 network support is that new switches (hardware) will be required. One reason is that existing ISDN switches are based on circuit-switched services, whereas B-ISDN technology is based on fast packet fixed cells.

B. OTHER DIGITAL TECHNOLOGIES

1. Frame Relay

Frame Relay, based on CCITT Recommendation I.122, is similar in concept to ATM and is exemplary for bursty traffic. It is a fast packet-switching technology offered by ISDN (using LAP-D) as an improved service over X.25. Frame relay is mostly used for interconnecting LANs/WANs. One of the most important features of frame relay is its ability to provide increased throughput by eliminating elaborate step-by-step error detection and retransmission. Essentially, at layer 2 frame relay determines if there is a valid frame to transmit. If so, it verifies the validity of the Data Link Connection Identifier (DLCI) which is a virtual circuit number corresponding to a particular destination. If it is valid then it delivers it to layer 3 for transmission. On the other hand, if there is an invalid frame or DLCI at layer 2, then the entire frame is discarded [Ref. 40:p. 18]. One of the reasons for the low overhead of frame relay is its dependence on end-point devices (e.g., PCs, workstations, and hosts). These intelligent devices can detect and recover from loss of data in the network and thus eliminates the error recovery as would be required at layer 3 for X.25. Frame relay transmits variable

length packets (called frames) and differs in structure from the fixed 53-byte cells of ATM. Frames may vary greatly in length up to some degree limit, usually 1000 bytes or more. When information is carried, frame relay makes a very small change to the frame structure. It redefines the header at the beginning of the frame. The 2-byte field of the frame header consists of an address field and a control field.

Many vendors have started to produce and deploy frame relay products. Most frame relay services, use a mix of frame relay attributes (proprietary) caused by the lack of definitive CCITT specifications [Ref. 38:p. 3]. The test results on a four-node frame relay network revealed that there was no standard implementation of frame relay by equipment manufacturers and consequently, resulted in significant interoperability problems [Ref 38:p. 3]. The frame relay standard is so broad that it allows vendors great latitude in how they implement frame relay in their products. Regardless of these inconsistencies and concerns, much of industry is moving rapidly towards frame relay vice SMDS. Regional Bell Operating Companies (RBOCs) are considering frame relay services as an intermediate data offering, something to fill the gap between their switched 56 kbps and broadband services such as SMDS [Ref. 39:p. 11]. There are two primary reasons for this shift: frame relay's long-distance availability and the improving infrastructure of the RBOCs. Because frame relay is offered as ISDN service, it is able to span great distances. Additionally, the infrastructure of the phone companies is rapidly becoming fiber optic allowing frame relay to work efficiently at much lower error rates (10^{-10} bit error rate [BER] versus the copper BER of 10^{-6}) [Ref. 14:p. 3-12]. The

use of one technology over another will ultimately depend on the users application and the availability of the service.

2. Switch Multi-Megabit Data Service (SMDS)

SMDS is a connectionless, high performance, public packet-switched data service designed to interconnect computers and local area networks, over wide geographical areas. Information is transferred in a short and bursty manner with speeds of 1.544 Mbps and 45 Mbps. Sometimes used synonymously with MAN, SMDS is based on the IEEE 802.6 standards Distributed Queue Dual Bus (DQDB). The motivation for SMDS is driven by the need to support data exchange between geographically separated users and the demand for increased high-bandwidth applications. As such, SMDS extends the scope of FDDI, Token Ring, and Ethernet by allowing wide area, high performance interconnection of these networks to support high bandwidth applications [Ref. 41:p. 33]. The connectionless service offered by SMDS has an advantage over current connection-oriented services because no connection is established between the end users. A packet of data is propelled from one piece of terminal equipment to the other. It is up to the intervening network to route the packet to the destination. Because this is a connectionless technology, as many are today, an end-to-end transport protocol must be used to provide reliability and control [Ref. 40:p. 20]. This might include TCP/IP, ISO/IP or some vendor-specific proprietary protocol. There are two prominent features of SMDS technology: (1) security and (2) its similarity to the ISDN standard numbering scheme. To provide confidentiality and security, all of the bandwidth within an SMDS channel is dedicated exclusively to one customer, no

sharing is done. This scheme should provide suitable protection for interexchange of data between MILDEPs applications. In terms of ISDN standardization, SMDS uses the CCITT ISDN numbering scheme standard (E.164) [Ref. 42:p. 1]. This will make it easier to transition to broadband ISDNs as they are deployed. However, one limitation hindering full-scale deployment, within the context of narrowband ISDN, is its lack of long distance availability. Interexchange carriers (IXCs) are not yet equipped to provide SMDS between the local access transport areas (LATAs) on a regional basis. Full deployment can be expected by late 1992 or early 1993. While initial deployment of SMDS will be at speeds of 1.544 Mbps, some commercial carriers will field the service at 45 Mbps. Eventually, SMDS will operate at SONET speeds of 51.84 Mbps and up to 2.488 Gbps. [Ref. 43:p. 7] Table V-2 on the following page shows a comparison of packet, frame, and cell (including SMDS and B-ISDN) switching [Ref. 44:p. 22].

TABLE V-2
COMPARISON OF PACKET, FRAME AND CELL SWITCHING

Switching Service	Packet Length	Packet Thru-put Per Second	Switch Level	HW/SW Switching	Error Handling	Circuit Type	Traf-fic Type
Traditional Packet Switching	Variable (Packet)	100-30k	Layer 3	Software	Yes	Analog	Data
Fast Packet/Frame Relay	Variable (Frame)	10K-100K	Layer 2 and 3	Software	Detection Only	Digital	Data
Fast Packet/Cell Relay SMDS, B-ISDN (ATM)	Fixed (Cell)	100K-100M +	Layer 1 and 2	Hardware	Detection Only	Fiber	Data Voice Video

3. Fiber Distributed Data Interface (FDDI)

FDDI is a high-speed, 100 Mbps, general purpose LAN interface standard optimized for multimode optical fiber, but extensible to support alternative media. Developed under the edicts of the ANSI, FDDI offers an industry-standard solution for organizations that need flexible, robust, high-performance, multi-vendor networks. FDDI is based on multimode (62.5/125) fiber optic media connected to form dual, counter-rotating rings [Ref. 17:p. 73]. It is intended to meet needs ranging from high-speed LAN to small metropolitan area networks (MANs). Up to 500 stations may connect into a single ring, with up to two kilometers between stations, provided total ring circumference does not exceed 100 km. FDDI does not use the priority/reservation scheme of 802.5 for reasons of efficiency. Accordingly, the FDDI MAC frame is the

same as that of 802.5 except that there is no access control field in the FDDI frame [Ref. 18:p. 429]. The inclusion of FDDI in GOSIP has been slowed due to delays in the Station Management (SMT) standard. SMT interfaces to the physical and link layers of FDDI to control initialization and configuration of the ring, as well as reconfiguration around faults and management services to higher layer management protocols. [Ref. 17:p. 73] FDDI has been slated for inclusion in GOSIP Version 3.

4. Synchronous Optical Network (SONET)

Unlike frame relay, FDDI, and ATM, SONET is not a telecommunications service in itself. Instead, it defines a standard interface between optical networks upon which broadband services are provided. The primary goal of the SONET standard is to define a synchronous optical hierarchy with sufficient flexibility to carry many different capacity signals. It operates at a basic signalling rate of 51.84 Mbps, called Synchronous Transport Signal 1 (STS-1). It defines two aspects: (1) multiplexing formats greater than DS-3[12] and, (2) optical signal formats corresponding to digital signals. A frame structure of the SONET STS-1 format is shown in Figure 26 [Ref. 45:p. 6]. By featuring its own optical carrier hierarchy, data rates up to 2.488 Gbps are achievable. Related optical character (OC) signal designation and line rates are described in the table below.

[12]Digital Signal (DS) channel rates are in multiples of 64 kbps and based on the North American Signal Digital Hierarchy (SDH). A DS-3 is equivalent to a data rate of 44.736 Mbps.

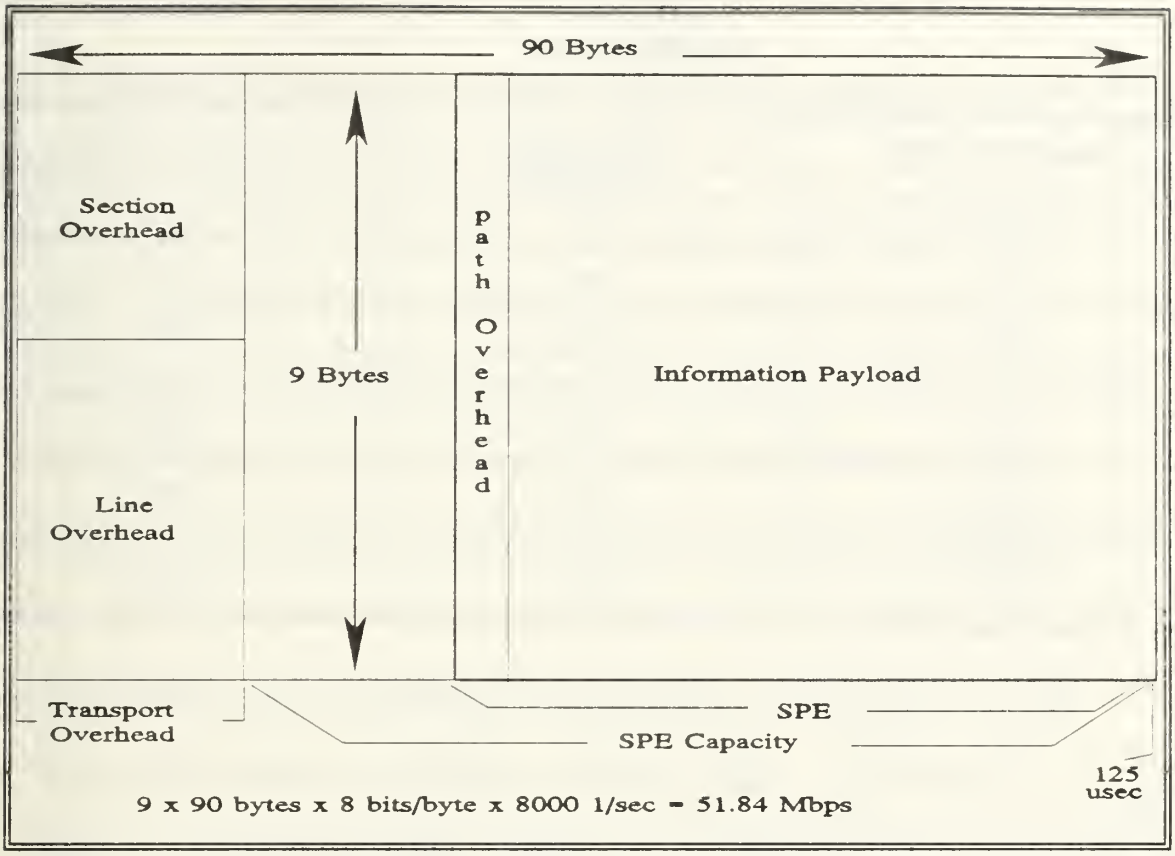


Figure 26
SONET STS-1 Format

TABLE V-3
SONET RATES

Signal Designation	Optical Signal Designation	Line Rates (Mbps)
STS-1	OC-1	51.84
STS-3	OC-3	155.2
STS-9	OC-9	466.56
STS-12	OC-12	622.08
STS-18	OC-18	933.12
STS-24	OC-24	1244.16
STS-36	OC-36	1866.24
STS-48	OC-48	2488.32

Because of design differences between T-3 and SONET, a T-3 switch cannot function as a SONET switch, although a SONET switch can function as a T-3 switch [Ref. 14:p. 87]. Because SONET is an emerging international standard like other evolving technologies, it is not expected to be available for deployment on a large scale soon. There are implementation concerns involving switch incompatibilities. Standards committees are working to define the capabilities of transport and switching system preliminary requirements. The target of this work is to provide switched services over SONET/ATM transport using signalling based on extensions to the Q.931 ISDN protocol [Ref. 37:p. 39]. The GOSIP FIPS will also evolve to account for the availability of SONET [Ref. 21:p. 61]; however, the date is unknown.

C. SUMMARY

Advances in terminal technology, optical fiber transmission, and switching technology, together with a rising demand for information-rich services, are accelerating the telecommunications environment through ISDN to B-ISDN before the end of the century. Like ISDN, it will be a number of years before the full spectrum of B-ISDN is available, but some communities expect mature standards by late 1992. At present, every major manufacturer has prototype broadband ISDN switching technology; and the additional functions needed to complete the definition might easily be added later [Ref. 37:p. 42]. GOSIP will evolve to account for the availability of B-ISDN. The use of B-ISDN will be based on two fundamental requirements: (1) specifications enabling multi-vendor interconnection compatibility between terminal equipment and switching equipment and (2) specifications enabling multi-vendor interconnection compatibility between switching equipment [Ref. 21:p. 61].

VI. CONFORMANCE GUIDELINES AND TEST PROCEDURES

A. BACKGROUND

Differences often exist between networks and between systems connected to these networks. These differences must be resolved by the MILDEPs in supporting C^3 activities. Developing and promulgating the open system standard in itself is not sufficient to ensure compatibility between networked systems. Conformance guidelines establish the foundation for providing assurance of compatibility between the many diverse computers and networks. Within GOSIP, this form of assurance is provided by conformance test methodologies established by the NIST. GOSIP addresses several layers of testing which are designed to overcome implementation and incompatibility problems associated with open COTS products. They include conformance, performance, interoperability, and functionality testing. Standard test suites have been developed for conformance to the standards and interoperability between systems. However, many large C^3 systems environment are manifested with unique requirements that cannot all be represented by standardized test suites. Therefore, Service- and organization-specific certification schemes must be developed. This chapter concentrates on several aspects of conformance testing. Sections B, C, D, and E address conformance test policies, conformance test laboratories, conformance test process, and conformance test suites, respectively. Conformance testing alone, however, is not entirely encompassing to ensure adequate interoperability. There should be clear guidance at the

DoD level to test beyond the level of conformance testing at the lower layers of the protocol model. This involves interoperability testing and is the second most important category of testing needed for compatibility between joint C^3 systems. The last two sections discuss the DoD ISDN testing policy and three classes of testing beyond that of conformance testing.

B. ORGANIZATIONS ESTABLISHING TEST POLICY

1. National Institute of Standards and Technology (NIST)[13]

NIST is responsible for encouraging national standards and has precedent procedures to ensure open and fair treatment of all interested parties. More specifically, they are responsible for producing the conformance tests and delivery mechanisms [Ref. 46:p. 7]. Under procedures developed by the Computer System Laboratory (CSL) and the National Voluntary Laboratory Accreditation Program (NVLAP), NIST establishes testing policy guidelines based on evaluating abstract test suites, means of testing (i.e.. test systems), and accredits conformance test laboratories as well as interoperability test laboratories. NIST is attempting to satisfy federal government requirements with standards that, as far as possible, are compatible with international standards [Ref. 18:p. 25]. NIST uses the assistance of the NIU-Form, COS, and other standards bodies to help create the policies and procedures for GOSIP [Ref. 17:p. xi].

---

[13]See Appendix C for organizational description.

2. North American ISDN Users' Forum (NIU-Forum)

The NIST sponsors the NIU-Forum. Its involvement in the forum activities is crucial to promulgating open systems. The NIU-Forum is the users' voice in ISDN implementation and applications. The four major philosophies driving the forum are: user services, interoperability, open systems, and conformance testing. While the forum recognizes all four as essential concepts, interoperability and conformance testing are key issues in providing true user transparency in communications across diverse environments. The NIU-Forum agrees that interoperability will be expected across facilities never before encountered such as transmission (e.g., fiber, cable, copper), upward and downward compatibility across generations of equipment and software, continuity through transitions, legal/copyright protection, and technical concepts (e.g., OSI, ISDN) [Ref. 46:p. 7]. The NIU-Forum charter and the NIST role is subjected to close scrutiny by the Department of Commerce and Congressional committees. As a result, NIST is encouraged to sponsor groups such as the NIU-Forum and seek national consensus on critical national standards efforts.

3. Corporation for Open System (COS) International

COS International, created in early 1986, is a nonprofit joint venture of more than 100 major data processing and data equipment suppliers. The following quote describes its mission [Ref. 17:p. x]:

> to provide a vehicle for acceleration of the introduction of interoperable, multi-vendor products and services operating under agreed-to OSI, ISDN and related international standards to assure widespread customer acceptance of an open network architecture in world markets.

COS's most important activity is the development of a single consistent national policy for information technology testing, test facility, and certification procedures [Ref. 19:p. 12]. In pursuit of this goal, COS works with NIST under a cooperative venture agreement, to help create policies and procedures for GOSIP. COS initiatives and programs build up the market for open systems products and services and break down the barriers to the Open System Environment [Ref. 17:p. x]. The creation of an Open Systems Model allows organizations such as NIST, X/Open, and Open Software Foundation (OSF), to participate to provide guidance. Collectively, these organizations work to promote the wide-spread deployment of open system standards through both policy guidelines and the use of test laboratories.

C. TESTING LABORATORIES

Conformance (or interoperation) testing has been undertaken both in private industry and at NIST to substantively increase the likelihood of interoperability. Testing to standards plays a significant role in promoting interoperability. This is true in both commercial applications as well as applications within the C^3 communities. Testing laboratories at the international, national, private, DoD, and service levels have been established to accelerate open systems product availability and to uncover product deficiencies. However, DoD or MILDEP testing is more aimed at the latter. Conformance testing can also be done using first- or third-party laboratories. The following subsections provide an overview of some of the laboratories available at the national, private, DoD and MILDEP levels.

1. NIST Computer Systems Laboratory (CSL)

CSL is a major science and engineering research component of the NIST. Their charter includes the development of standards, guidelines, and test methods for computer systems and networks. CSL is charged with the overall responsibility for product testing and certification activities for both conformance and interoperability testing. The actual execution is a joint government-user-vendor-enterprise. In its role as implementation coordinator for the GOSIP program, the CSL at NIST has instituted a GOSIP product testing and certification program. One of the primary objectives of the testing and registration program is the establishment and maintenance of a list (known as a register) of certified GOSIP-compliant products. Suppliers seeking to have products placed on the register are required to submit them for various forms of examination and testing. Products that successfully demonstrate GOSIP compliance during the testing and registration process are placed on this register. A second objective is to increase the likelihood of interoperation of GOSIP-compliant products.

CSL sanctions the use of first- and third-party test laboratories. A first-party laboratory is operated by the product supplier and is authorized to test only "in-house" products. This is a "self-testing" but under closely monitored conditions. Third-party laboratories are operated by independent organizations of the supplier of the product. It is usually a profit-oriented operation and its results are monitored by the NVLAP. Any distrust or misrepresentation results in withdrawal of CSL accreditation. Within CSLs laboratory-based research program, they continue to develop test and measurement

methods to evaluate conformance of products to standards and the interoperability of the many data communications components [Ref. 47:p. 1].

2. COS Conformance Test Laboratory

In addition to promoting the acceleration of multi-vendored interoperable products, COS also supports and provides conformance test certification. COS has created a program to certify vendor COTS products under a program called the COS Mark Program. The program is a user-vendor sponsored OSI/ISDN product certification program whose objective is to identify and distinguish those products in the marketplace that meets COS requirements. COS mark certification is based on testing performed within the COS laboratory. There are three points that this level of testing should produce [Ref. 17:p. xii]: (1) a commitment that any interoperability problems will be resolved between COS and the vendor, (2) a level of confidence that the product has been rigorously conformance tested, and (3) a level of comfort that COS Interoperability Analysis Service (IAS) experts are available to resolve interoperability issues at no cost. Much of the GOSIP testing policy is based on the COS Mark Program. In fact, COS has contributed several of the test and means of test (MOTs) found in the GOSIP register. With the procurement of COS Mark licensed products, in addition to GOSIP compliance, it assures that vendor products have been subjected to rigorous conformance testing.

3. DoD Joint Interoperability Test Center (JITC)

The JITC is a DoD-level interoperability test laboratory. Located in Fort Huachuca, Arizona, this organization has been selected by NIST as the testbed for

interoperability testing of joint C^3 systems. The JITC has the charter, facilities and capability to provide the CINC's, MILDEPs, agencies and others a real world look at the degree of interoperability within their systems. Their role include registering products and laboratories that meet GOSIP requirements, maintaining those registers and testing GOSIP test tools [Ref. 48:p. 18]. JITC's network is rapidly expanding to accommodate interoperability testing from numerous and diverse locations. The equipment does not have to be physically co-located at Fort Huachuca to perform testing which reduces additional resource expenditures. NIST and DISA expect the lab to operate on a cost-reimbursable basis. It will use a tiered rate structure, reflecting four types of client organizations: DISA, DoD, federal and commercial. Currently JITC is the sole agency that test GOSIP testers and is one of several government agencies planning to become an accredited agency for conformance testing. JCS highly recommends that testing at JITC be made an integral, early milestone in the development of *all* C4I systems regardless of cost, size, application, etc [Ref. 49:p. 7]

Although the JITC will be used primarily for GOSIP testing, JIEO (formerly JTC3A) believes that the centers facility could be expanded to promote ISDN testing as well. But JIEO conveys that there is no capability or fully developed conformance test suites to perform comprehensive "ISDN" product testing yet. JIEO is, however, planning to conduct ISDN testing along with analyzing test tools. Connection approval will be granted by the Center for Engineering (at DISA) once certified compliant. It is unclear exactly what level of testing the center will perform or when the conformance test abstracts will be available with respect to ISDN. JIEO expects that the NIU-Forum

and other chartered organizations may have a full suite (layers 1-3) by the Fall 1993 [Ref. 50]. Despite the availability of existing testbeds like JITC, many of the MILDEPs have developed their own test laboratories.

4. MILDEP Testing Programs

MIL-STD 188-194 suggests that testing be performed at all levels specified by GOSIP: conformance, interoperability, functionality, and performance. While the JITC can support testing, an examination was made as to why individual laboratories by the MILDEPs were necessary. The following is a result of that analysis:

- Scheduling and allocation of available test resources at Ft Huachuca and the geographically separated organizations to support the test.
- Service-unique requirements or organization policy. Some services feel that their test needs for ensuring conformance and interoperability is best served within their own service. For instance, the Air Force's GOSIP Transition Plan makes it clear that they will be responsible for performing interoperability testing between GOSIP systems of different vendors, with existing systems, gateways, etc. prior to implementation. They further stated that the responsibility for Air Force testing cannot be placed on any organization outside the Air Force, for it is solely responsible for the Air Force's architectures and communications-computer systems [Ref. 51:p. B-6].
- Some system processing environments are quite unique and, therefore, many of these operational systems do not have a requirement to interface with or interoperate with C^3 systems. As a consequence, they are not tested.

a. Air Force's Test Environment

The Air Force has a test facility located at Barskdale AFB, Louisiana called the Air Force Model Base Program Office. Under the auspices of the Technical Integration Center (TIC), located at Scott Air Force Base, Illinois, the test bed's primary

mission is to analyze the impact of base-level systems prior to worldwide deployment. As seen in the Air Force's architecture (Chapter II), the base infrastructure consists of diverse local area networks and computer systems, ISDN, point-to-point links, and other types of networked topologies. The Model Base facility at Barksdale AFB is set up to simulate a typical Air Force Base processing environment in support of these topologies. Once interoperability within a controlled environment has been established and functionality and performance have been verified, operational testing within an actual base environment will be their responsibility. The Air Force believes that the process of testing in a controlled environment and then in an operational environment will greatly improve the likelihood of maximum system interoperability. [Ref. 51:p. B-6].

b. Navy's Test Environment

The Navy has established its test bed at the Navy Yard located in Washington D.C. The testbed consists of a team of developers and system engineers. The primary mission of the test environment is the testing of OSI products and to support the migration toward open systems. The feasibility and testing of ISDN is being explored by the Navy but not at the OSI laboratory. One initiative is the DoD ISDN Trail in FY 93 where China Lake Naval Air Station will be participating. They have installed is a Northern Telecom DMS-100 ISDN switch which will connect onto the trail backbone.

c. Army's Test Environment

The Army has an ISDN research and development activity (ARMICS) located at Georgia Tech, Atlanta, Georgia. Their primary mission is the development

of and testing ISDN-based applications. However, previous experiences with ISDN began at the USAISC-MICOM located at Redstone Arsenal, Alabama. They were the first trial site for the Army's ISDN efforts. The trial began in March 1988, with the installation of an AT&T 5ESS leased from Bell South, and ended in January 1991. The primary purpose of the trial was to demonstrate and support base-wide ISDN applications. They have now moved into a full-deployment of ISDN for base support. USAISC-MICOM is furthering their trial efforts by investigating evolving technologies such as FDDI, SMDS, and frame relay. An effort began in February 1992 evaluating the use of SMDS and frame relay. Using AT&T routers connected to the existing AT&T 5ESS, they wish to show application usage of these technologies and potential trade-offs. The trial concludes in December 1992 with the publication of a test report. [Ref. 52] Future efforts involving ISDN testing will include the Army location at Fort Huachuca, Arizona.

The manifestation of interoperability problems is ever present. Within the military especially, this is stimulated by issues such as limited resource availability, a narrow view toward non-parochial testing, and political issues within the services. It is envisioned that JCS involvement will infiltrate the services and encourage testing before these systems are deployed, unlike in Desert Shield/Desert Storm.

D. CONFORMANCE TESTING AND PROCESS

Since compatibility with standards cannot be determined visually, tests have been written to establish compatibility of products. These are called conformance test suites.

At the most general level, conformance testing analyzes potential OSI products to verify that it fulfills the requirements of a written standard. It verifies that an implementation acts in accordance with a particular specification, such as GOSIP. Conformance testing can be thought of as a unit testing specifically applied to functionality imposed by the relevant standards. The process by which to perform conformance testing has been established at the Federal level using three entities [Ref. 16:p. 47]: (1) standardized abstract test suites, (2) means of test (MOTs), and (3) fully accredited conformance test laboratories. Abstract test suites defines the criteria for test suite coverage. These abstracts will be used as the standard reference for the assessment of MOT [Ref. 52:p. v]. MOTs are used to actually perform the conformance testing. To be GOSIP-compliant, the MOT itself must be NIST or GOSIP-certified. MOT encompasses all of the following [Ref. 17:p. 36]:

- The hardware and software support tools used to test (hardware platform, operating system, file management mechanisms, results analysis tools, etc.);
- The test engine (test driver and protocol analyzer);
- The executable test suite (the set of scripts used to achieve the purposes of individual tests); and
- The documentation (test procedures, verdict assignment guidelines, etc.).

Accreditation by NIST certifies that candidate laboratories are qualified to conduct GOSIP product testing. All three of these entities are contained in the GOSIP Conformance and Interoperation Test Registration [Ref. 53], which establishes the framework for the procurement of GOSIP-compliant products. In essence, the

conformance test process begins with a written test abstract and concludes with the System Conformance Test Report (SCTR). A description of conformance testing along with the testing process follows.

1. Description of Conformance Testing

Conformance testing of OSI protocols is an internationally standardized methodology[14]. The methodology consists of an examination of product's external protocol behavior to determine the extent to which it conforms to the standards--basically the "incorrect" behavior. The purpose of the methodology and framework is to simulate network environments that duplicates, to the extent possible, a real network. However, the protocol implementation being tested is exercised by a test engine running test scripts rather than a bona fide peer protocol. Figure 27 depicts a general description of how a system under test (SUT) is evaluated against a conformance test system [Ref. 17:p.34]. A single layer of the OSI protocol stack is tested using the services of the lower layers with have been tested previously and are, therefore, assumed to be correct. GOSIP conformance testing is distinguished in three essential ways. First, testing is conducted in an objective context independent of pressure from product developers and delivery schedules. Second, conformance testing is performed with extreme rigor. It utilizes state-of-the-art testing technology and is performed using procedures sufficiently detailed to maximize the likelihood that product conformance errors will be expected. Finally, conformance testing produces an audit trail that can be beneficial to both the product

[14]Defined in IS 9646, *Conformance Testing Methodology and Framework.*

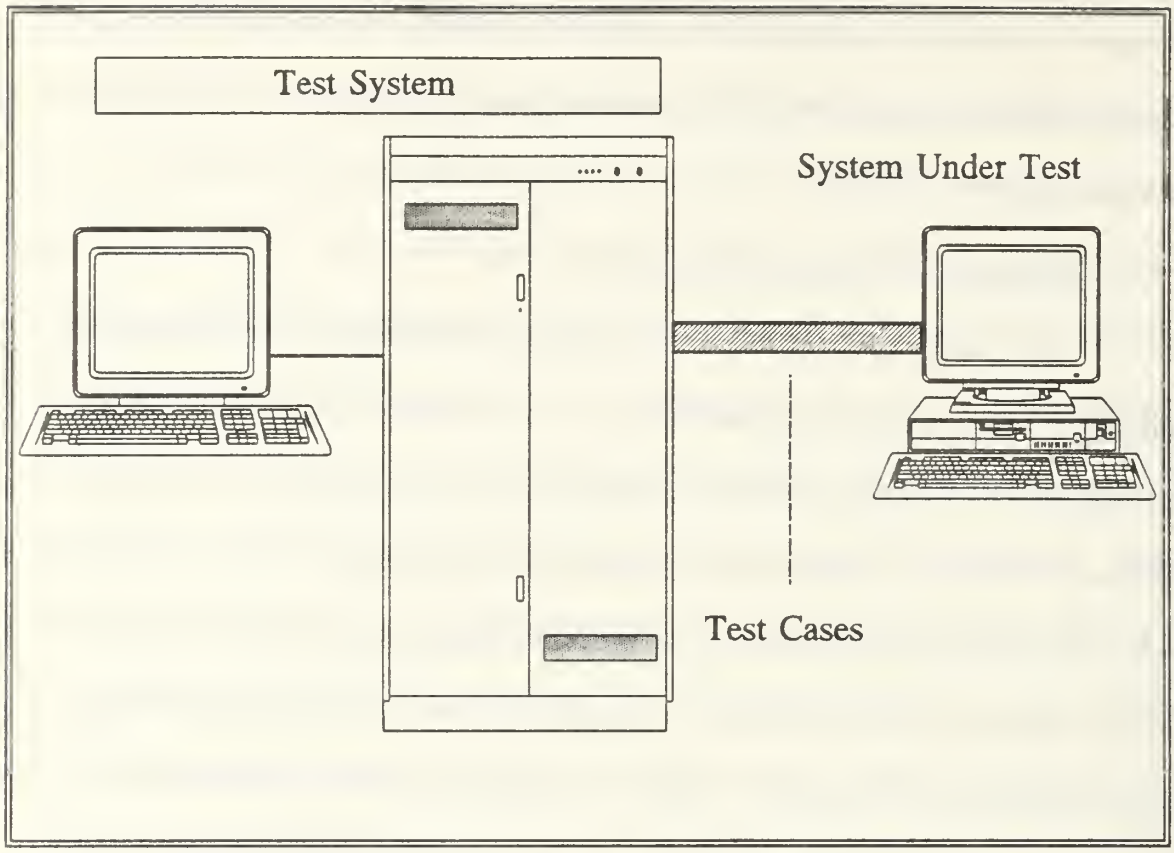


Figure 27
Conformance Testing

developer and the purchaser. It provides conformance test data and documented outcome of product testing.

2. Abstract and Executable Test Suites

Conformance test begins with an abstract test suite written so that multiple test equipment vendors may provide implementation of the test suite. A test suite is composed of individual test cases each of which describes the actions necessary to achieve one or more test purposes. The description of a test case is called an "abstract" when it is sufficiently generalized to enable it to be implemented on a number of test

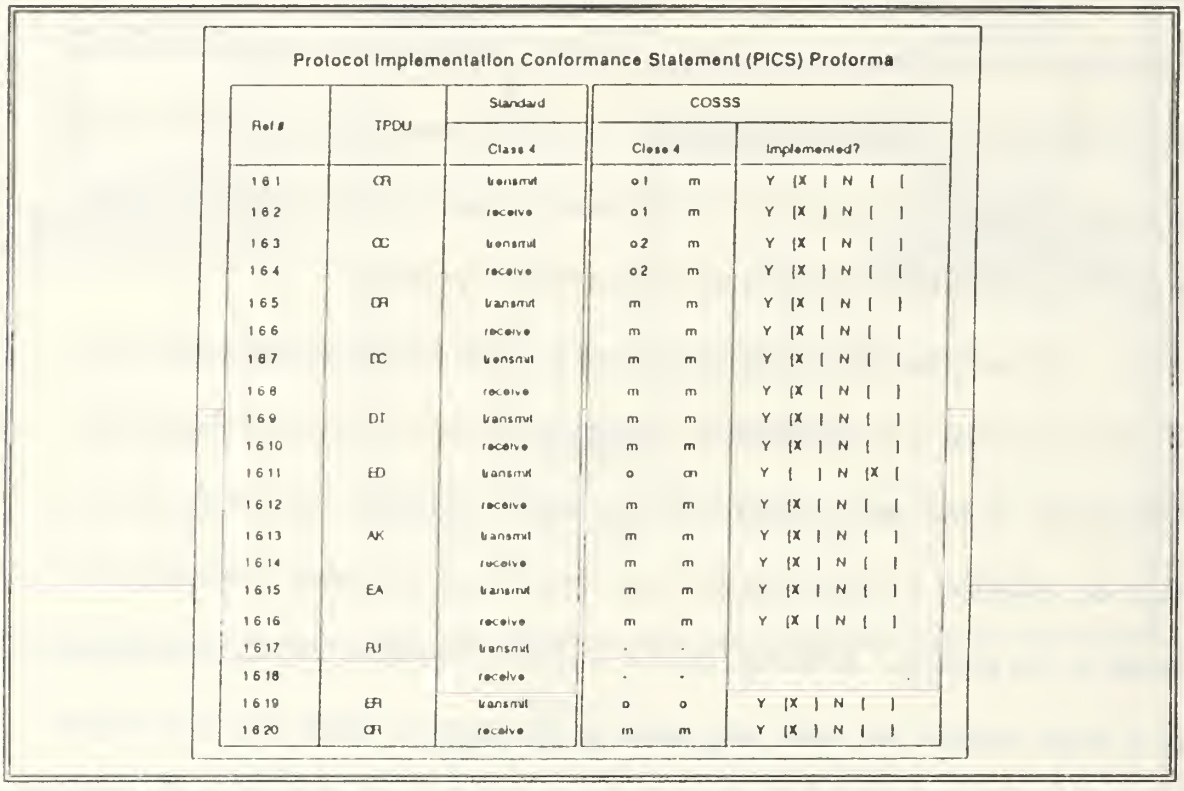
systems or in a number of different ways. The actual script used by a test system to achieve one or more test purposes is called an "executable" test case. Most, but not all, abstract test suites are written by committees of protocol experts under the auspices of international standards bodies such as ISO or CCITT. They are then refined on the basis of local protocol Implementor's Agreements. TP-4 is an example of a GOSIP protocol class with no standardized test suite. In such cases, several de facto abstract test suites may exist, each based on a different test system for that protocol.

All accredited MOTs must provide test coverage equivalent to that abstract test suite. The actual test cases executed by different MOTs may vary, but the functionality that the battery of test cases actually exercises must be the same. For an abstract test suite to be complete, it must contain at least one test case for each function/service provided by the protocol. However, the two different executable test suites developed from a single abstract test suite may differ in the depth to which they test various functions. The horizontal coverage may be identical, but the vertical coverage could still vary.

3. Protocol Implementation Conformance Statement (PICS)

A PICS is simply a formal questionnaire describing the protocol functions/services to be tested. Figure 28 is a representation of a filled-out PICS after completion of conformance testing [Ref. 17:p. 39]. The PICS is a concise listing of the protocol functions and services detailing the product's functionality. By its concept, the completed PICS serves two functions. First it allows the testing organization to perform a static assessment of the product. If the supplier checks "yes" for all mandatory

protocol elements, then the product passes static assessment. If the supplier checks "no" for one or more mandatory elements, the products fails static assessment. The second



Protocol Implementation Conformance Statement (PICS) Proforma

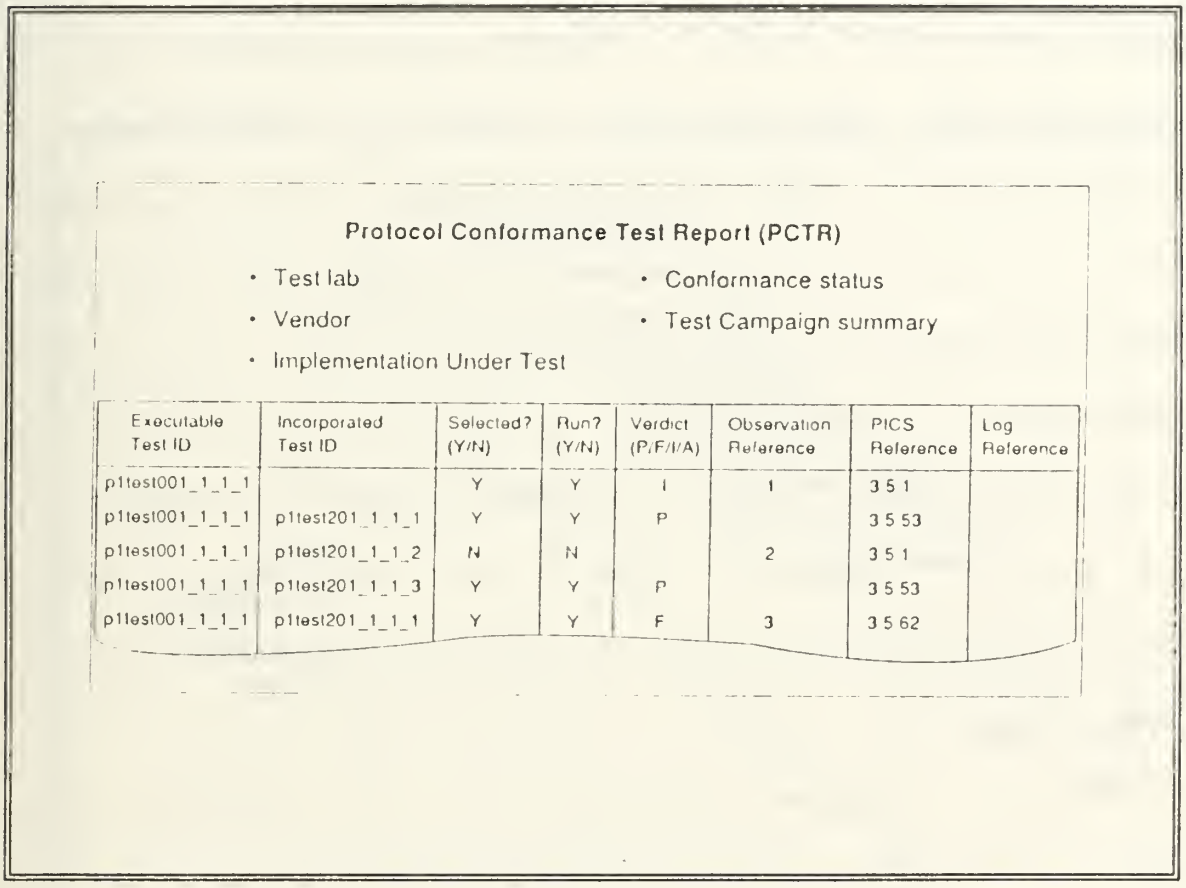
Ref #	TPDU	Standard	COSSS		
		Class 4	Class 4		Implemented?
1 6 1	CR	transmit	o 1	m	Y [X] N [ ]
1 6 2		receive	o 1	m	Y [X] N [ ]
1 6 3	CC	transmit	o 2	m	Y [X] N [ ]
1 6 4		receive	o 2	m	Y [X] N [ ]
1 6 5	DR	transmit	m	m	Y [X] N [ ]
1 6 6		receive	m	m	Y [X] N [ ]
1 6 7	DC	transmit	m	m	Y [X] N [ ]
1 6 8		receive	m	m	Y [X] N [ ]
1 6 9	DT	transmit	m	m	Y [X] N [ ]
1 6 10		receive	m	m	Y [X] N [ ]
1 6 11	ED	transmit	o	cn	Y [ ] N [X]
1 6 12		receive	m	m	Y [X] N [ ]
1 6 13	AK	transmit	m	m	Y [X] N [ ]
1 6 14		receive	m	m	Y [X] N [ ]
1 6 15	EA	transmit	m	m	Y [X] N [ ]
1 6 16		receive	m	m	Y [X] N [ ]
1 6 17	RJ	transmit	-	-	
1 6 18		receive	-	-	
1 6 19	ER	transmit	o	o	Y [X] N [ ]
1 6 20	CR	receive	m	m	Y [X] N [ ]

Figure 28
Protocol Implementation Conformance Statement (PICS)

function of the PICS is that it serves as a guide for test case selection by the test engineer. If an operational feature is indicated as not implemented, then the test case that exercises that function is "de-selected." In summary, PICS list omitted functionalities as well as any functionality which the supplier was reluctant about having tested. The PICS is currently the only way to easily catch disparities between two rival products.

4. Protocol Conformance Test Report (PCTR)

A Protocol Conformance Test Report (PCTR) is prepared upon completion of the conformance testing (e.g.,PICS). A PCTR is shown in Figure 29 [Ref. 17:p. 41]. The PCTR is a summary of the results of testing for a single protocol. A separate PCTR is prepared for each single protocol under test. For example in testing of the Message



Executable Test ID	Incorporated Test ID	Selected? (Y/N)	Run? (Y/N)	Verdict (P/F/I/A)	Observation Reference	PICS Reference	Log Reference
p1test001_1_1_1		Y	Y	I	1	3 5 1	
p1test001_1_1_1	p1test201_1_1_1	Y	Y	P		3 5 53	
p1test001_1_1_1	p1test201_1_1_2	N	N		2	3 5 1	
p1test001_1_1_1	p1test201_1_1_3	Y	Y	P		3 5 53	
p1test001_1_1_1	p1test201_1_1_1	Y	Y	F	3	3 5 62	

Figure 29
Protocol Conformance Test Report (PCTR)

Handling System (MHS), a PCTR is prepared for the reliable transfer service (RTS), P1, and P2 protocols. The PCTR can also contain any test that was de-selected as well as

the test engineer's comments about individual tests. More importantly, the PCTR will indicate the number of tests that resulted in inclusive or inconclusive verdicts.

5. System Conformance Test Statement Report (SCTR)

The SCTR completes the conformance test process. The SCTR is essentially a concatenation, or summary, of the conclusions reported in the PCTRs. Figure 30 is a general depiction of the SCTR [Ref. 17:p. 42].

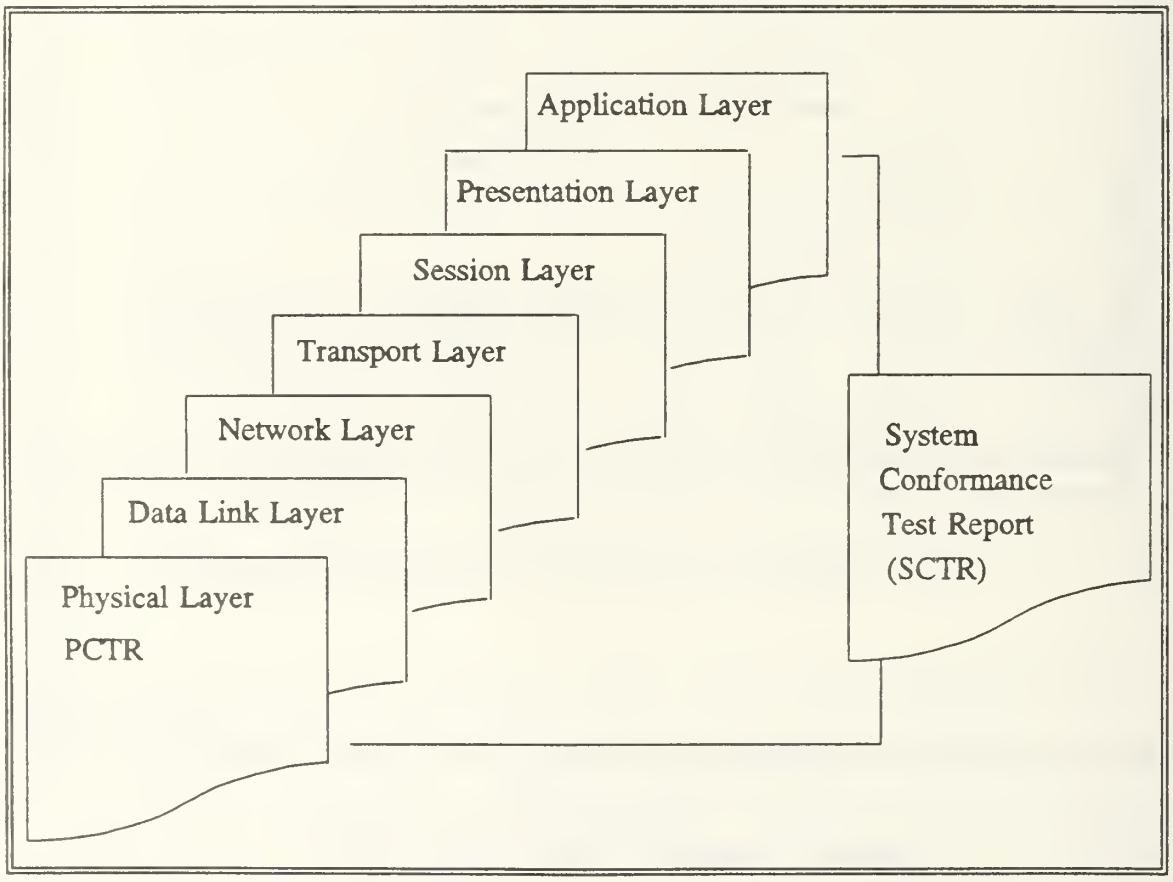


Figure 30
System Conformance Test Report (SCTR)

Products that have successfully met GOSIP compliance are then placed in various registers (e.g., test suites, test systems, etc). NIST has developed a single register called the Register of Conformance Tested GOSIP Products for use. Products successfully tested in an accredited testing laboratory against a registered MOT may be entered into that register [Ref. 16:p. 47].

E. CONFORMANCE TEST SUITES

Standardization is the basis of conformance testing. The NIU-Forum's Conformance Test (CT) specifications provide test suites to be used to verify the conformance of ISDN equipments to the designated specifications [Ref. 30:p. 5-1]. CT specifications are written in abstract form so that multiple test equipment vendors may provide implementations of the test suite. The ISDN Conformance Test specifications are developed by the ISDN Conformance Test (ICOT) Working Group, and its subordinate Expert Working Groups: the Abstract Conformance Test Group for Layer 1 (ACT1) and the Abstract Conformance Test Group for Layers 2 and 3 (ACT23). [Ref. 30:p. 5-1] The slow maturation of ISDN has caused delays in the development of full ISDN test parameters. The full suite of ISDN product conformance test parameters are still under development. The following subsections delineates available conformance test specifications for each of the ISDN physical, data link, and network layers.

1. Physical Layer Test Specifications

Layer 1 of the CCITT ISDN standard describes the physical interface from CPE to a public network (see Figures 18 and 19 in Chapter IV). ISDN Layer 1

Conformance Testing for the S/T interface is specified in NIU-Forum/IIW/ICOT-90-40. ISDN Layer 1 Conformance Testing for the basic rate U interface is addressed in NIU-Forum/IIW/ICOT-90-60 [Ref. 27:p. 3]. The BRI Layer 1 CT specifications provide the requirements for verifying equipment conformance at the lowest layer of the ISDN BRI user-network interface. CT specifications for PRI are currently under development by the NIU-Forum.

2. Data Link Layer Test Specifications

At Layer 2, a D-channel link layer protocol guarantees end-to-end error correction and retransmission. The Layer 2 CT specifications, for the BRI and PRI access arrangements, provide the requirements for verifying equipment conformance at layer 2 of the ISDN BRI/PRI. The ISDN test suite development process is aligned with ISO 9646, OSI Conformance Testing Methodology and Framework, Parts 1-3. The ISDN Layer CT specification defines the abstract test suites for LAP-D data link protocol. Its use is for ISDN terminal equipments attaching to the user side of a basic access interface [Ref. 30:p. 5-2]. The purpose of the abstract test suite is to provide the most complete protocol conformance test coverage as is possible, not to be completely exhaustive. The LAP-D test suite has many additional test cases for TEI management procedures and system related cases[15]. The CT layer 2 for the PRI is pending.

---

[15]These procedures are addressed in the body of the CCITT Recommendation Q.921-1988 but not in the CCITT Recommendation Q.921-1988 state transition tables.

3. Network Layer Test Specifications

ISDN Layer 3 provides D-channel signalling protocols that are used to establish and route voice and data calls. The NIU-Forum has the charter for its development and testing, and is in the process of determining the test specifications requirements. Hence, the ISDN test specifications at this layer are not available at the moment. Table VI-1 provides a consolidated list of available conformance test criteria developed thus far by the NIU-Forum.

TABLE VI-1
NIU-FORUM CONFORMANCE TEST SPECIFICATIONS STATUS

Description	Reference Point	Conformance Test Description	Status
Layer 1 (BRI)	S/T	NIU-Forum/IIW/ICOT-90-40	
	U	NIU-Forum/IIW/ICOT-90-60	
Layer 1 (PRI)	S/T/U		In Progress
Layer 2 (BRI)	N/A	NIU-Forum/IIW/ICOT/ACT-91/22.2 V1.2	
Layer 2 (PRI)	N/A		In Progress
Layer 3	N/A		Both BRI and PRI in Progress

F. DoD ISDN CONFORMANCE TESTING

Since C^3 communities use both national and international carriers, incompatibilities are imminent. The need for product testing of ISDN COTS is evident. There are two areas of ISDN incompatibilities. The first is that carriers and central office switch makers in different countries are working with various standards for connecting CPE to

the public network. Those differences have arisen because of the range of options in CCITT ISDN standards. The other major incompatibility is that carriers are not yet equipped to handle ISDN D-channel transmissions. [Ref. 16:p. 110] However, there is no clear DoD-wide policy mandating ISDN conformance or interoperability testing at the network-to-network (SS7) level. The lack of testing at this level could lead to catastrophic consequences. One such repercussion is demonstrated by the AT&T SS7 blackout that crippled the Pacific and Atlantic regions in June 1991 [Ref. 54:p. 30]. The outage affected local voice communications, long distance traffic and millions of subscribers including VPNs. A similar AT&T outage also occurred in January 1990 [Ref. 54:p. 30]. These types of outages can affect communications across the MILDEPs which rely on common carriers for ISDN backbone services (including SS7). The local networks of the Bell companies are between 25% and 30% equipped with SS7 software. At the independent telephone companies, the percentage is somewhat higher, while at IXCs such as AT&T, MCI, and Sprint, the networks are nearly 100% SS7-based. End-to-end user services are totally dependent on these companies to establish a uniform signalling path over multiple SS7 networks.

The critical components of an SS7 network (STPs, SCPs, and SSPs) must communicate together effectively and preferably efficiently. The Federal Communications Commission (FCC) has encouraged comprehensive SS7 testing by more than 30 telecommunications industry organizations, including local and IXCs as well as equipment makers [Ref. 32:p. 15]. Although, interoperability testing between ISDN switches from a variety of vendors is outside the scope of GOSIP specifications [Ref.

55:p. 3], the NIU-Forum has efforts underway to address issues of switch-to-switch interoperation [Ref. 22:p. 61]. Even with the development of standardized test suites, however, it would be nonsensical to expect a fully interoperable ISDN across the broad spectrum of C^3 systems.

Another issue affecting the C^3 community is the lack of accredited ISDN conformance test laboratories at federal, DoD, or service level. GOSIP Version 1 laboratories were identified in late 1990. However, GOSIP Version 2 that includes ISDN does not identify any laboratories accredited to perform conformance testing. Hence federal agencies and organizations are left without the test systems and test cases required for conformance testing [Ref. 16:p. 47]. The development of additional conformance specifications and specifications beyond the standard conformance test level will therefore be needed.

G. BEYOND CONFORMANCE TESTING

There are three additional categories of testing that is important to support requirements such as robustness, flexibility, modularity, etc. They include interoperability, performance and functionality testing. While all three categories are contained in GOSIP Version 2, it only provides standardized test criteria for interoperability. The next three subsections provide an overview of these categories of testing.

1. Interoperability Testing

Interoperability is perhaps the most important to the successful interoperation (or interoperability) of joint C^3 systems. Interoperability testing is designed to detect incompatible configuration options and to simulate the real-life conditions under which the vendor's products will be seen. In actual testing, the focus is to ensure that a system under test (SUT) has the ability to interoperate with a reference implementation. A reference implementation is a real embodiment of the OSI standard. The system under test, shown in Figure 30 [Ref. 17:p. 35], consists of at least layers 1 through 3 and may involve as many as all seven protocol layers. Unlike conformance testing, where one layer is tested at a time, interoperability test all layers at once, but the scenarios are designed to ensure adequate coverage of specified functionality. Interoperation testing in later versions of GOSIP will identify problems attributable to such factors as mistakes and ambiguities in the standards, incompleteness of the standards, and application-layer incompatibilities not addressed in the standards. Since OSI vendors are building products to operate with implementations developed by others, it is in the interest of both the vendor and the agency to duplicate as closely as possible the environment in which the product will be used prior to acceptance. CSL policy mandates that conformance testing be a prerequisite for interoperability testing [Ref. 17:p. 34].

2. Performance Testing

A second classification of testing is performance testing. Some organizations have certain architectural features that are outside the scope of standardized test suites.

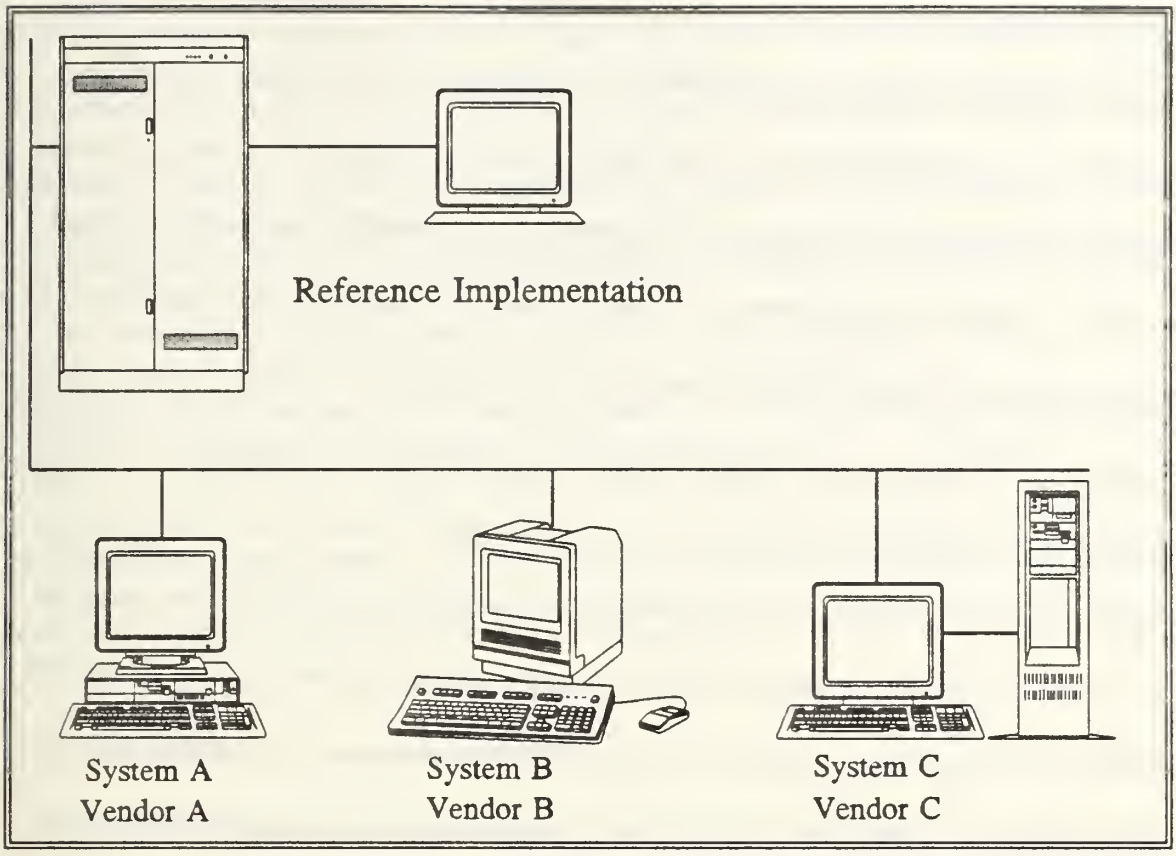


Figure 31
Interoperation Testing

For example, performance requirements may necessitate the location of certain protocol layers in a communications processor. GOSIP only requires that a protocol behave in a specified manner and does not address such design issues. No government-wide mechanism exist for features of this kind. [Ref. 17:p. 35] There are several forms of performance. One such form, important to C^3, is the overall system performance. System performance is usually described by a combination of parameters which have meaning only in terms of the system's functions. In the cases of sensors such as radars or infrared detectors, performance may be specified in terms of maximum detection

range for some given target cross section. Performance of communications channels is generally specified in terms of intelligibility or digital error rate for a set of conditions, bandwidth to be transmitted (or the equivalent in terms of signal waveforms), channel length, and the noise and attenuation (with distortion if applicable) which will exist [Ref. 3:p. 270]. Even the performance of general-purpose computers have performance characteristics. To estimate a given computer's performance in millions of instructions per second (MIPS) in a given application, not only must the statistical "mix" of instructions to be executed be defined but so must statistics of other tasks such as access to input/output and storage devices. Currently performance is not standardized under the scope of the OSI Reference Model. NIST is working to develop performance evaluation guidelines for GOSIP; not standards. The guidelines are estimated for completion in late 1990 or early 1991 [Ref. 17:p. 31]. Federal agencies may compare performance data, produced by vendors or research organizations, against agency requirements. The NIST may provide advice on realistic performance requirements given certain technological considerations. In addition, users need to determine the performance requirements pertinent to their particular situation. The NIST is developing performance metrics and benchmarks for certain GOSIP application. [Ref. 16:p. 46]

3. Functional Testing

GOSIP does not impose a "look and feel" onto user systems. Many of these requirements (e.g., graphical user interfaces) are embedded vendor-proprietary implementations. GOSIP mandates, for each protocol, a minimum set of functions to meet general government requirements; not features such as graphical user interfaces.

In many instances, additional functions might be supported within the NIST Workshop Agreements and/or the protocol standard. An agency must determine and specify what additional functions are required. Likewise they should also ensure that the vendor products proposed meet all functional requirements of that agency, regardless of whether or not those additional functions are subject to standardization. [Ref. 16:p. 46]. Although GOSIP does not discourage autonomous "look and feel" capabilities or user friendly functions, their unique implementations must not interfere with GOSIP interoperability requirements. In late 1991 or early 1992, the NIST will provide functional evaluation guidelines for users; not standards.

H. SUMMARY

GOSIP addresses several layers of testing--conformance, performance, interoperability, and functionality testing. However, test suites standards are difficult to write and have to be accepted by the vendor community as accurate and consistent with the standards. Conformance testing, by itself, does not ensure that an OSI protocol suite will work correctly. No conformance test can possible test all perturbations of a network's behavior or protocol errors. In addition, the likelihood of detecting all errors are further hindered by the design of conformance testing itself. Conformance testing is designed to test single layers. Because some vendors merge the functionality of two or more layers in a protocol implementation, it is difficult to determine the incorrect behavior of an implementation. The unique requirements of a C^3 community puts additional demands on testing. Organizations and testing laboratories at almost all levels

are available to assist in testing. At the joint level, the JITC has been designated as the testbed for interoperability testing of joint C^3 system, but predicated upon testing to standards (conformance testing) first. Ultimately, conformance testing, succeeded by interoperability testing, will increase the probability that a product interoperates with other multi-vendored products.

VII. SUMMARY AND CONCLUSIONS

A. SUMMARY

The ubiquitous deployment of ISDN is slowly becoming a reality not only within this country, but also within the military. However, its full deployment is hindered by both the lack of standards and incompatibilities between ISDN equipment vendors. Many developers of COTS are incorporating proprietary functionality within their equipment (e.g., frame relay) due to the lack of definitive standard and the slowness of the CCITT assembly (work is conducted in four-year cycles) to gain a consensus on these evolving standards. Almost every major vendor and operating company offer ISDN products or ISDN services today. Bell Atlantic, for example, has a projected high percentage (90%) and NYNEX a low percentage (18%) of ISDN access for 1994 [Ref. 56:p. 4]. Although there is a lack of full ISDN conformance test abstracts, its deployment and supplemental technologies will require extensive testing. Test suites developed for ISDN will be "trial and error" because of the complexities and interpretation of standards. When these abstracts are fully developed, there must be a clear DoD-wide policy requiring network level testing. Although the JCS strongly encourages using the JITC for interoperability testing [Ref. 49:p. 7], it is unclear exactly what level of testing the center will perform or when the conformance test abstracts will be available.

There also exist an incompatibility at both the user-to-network and the network-to-network (signalling) levels. For example, at the user-to-network level, it was noted that

Northern Telecom's DMS-100 BRI channel is incompatible with AT&T's 5ESS, Siemems Information EWSD switch or Ericsson's AXE switch. Similarly, there are two implementations of SS7 standards by the vendor communities: CCITT and ANSI. Some operating companies have implemented both within their network while others only support one. The DCS is ANSI-based, deploying both AT&T and Northern Telecom equipment. This will cause significant interoperability problems at the IXCs supporting control signalling. Regardless of the rate of ISDN deployment, B-ISDN is the next generation of high-speed multimedia transport mechanism. Migration to B-ISDN is a major technological improvement over ISDN in terms of bandwidth capacity and its ability to accommodate evolving technologies such as FDDI, SMDS, SONET, and frame relay. The advantages of B-ISDN is only over-shadowed by cost in terms of new or enhancements to equipment. Some existing switching software, used by the MILDEPs or the DCS, may not be upgradeable to support fast-packet ATM technology. Those switches will most likely require a hardware upgrade. The existing copper wire infrastructures cannot support B-ISDN and as such will require replacement to fiber optics. To install fiber optics on existing installations may take major efforts. Like ISDN, B-ISDN technologies depend upon consistent implementation of an intricate set of standards, many of which are not resident in a particular product. B-ISDN technologies, as part of the DISN, will no doubt encounter the same growing pains as the deployment of ISDN today.

B. CONCLUSIONS

There are obvious advantages to the B-ISDN and cell relay ATM technologies proposed for the DISN. This includes bandwidth capacity, minimal delay, security (e.g., SMDS) and similarities to current ISDN technology such as the standard E.164 numbering scheme. There are likewise advantages to conformance testing. Although new and major upgrades to data communications must be certified GOSIP-compliant, conformance testing alone does not ensure full interoperability. No conformance test system can ensure that all errors in a protocol implementation will be detected. It does, however, increase significantly the probability that a product interoperates with other products. DISA recognizes the issues of interoperability and the need for conformance testing [Ref. 57]. The migration from the near-term and transition phases to the far-term DISN will rely heavily on todays ISDN COTS and ISDN lessons learned. The incorporation of ISDN in GOSIP Version 2 offers new challenges to users and exchange carriers alike. There is little doubt that interoperability problems will have a profound impact during these two phases. The kinds of interoperability problems associated with the far-term DISN may be less profound than in the previous phases. One reason is because the far-term DISN will be based on leased services provided by exchange carriers. This places the problems of interoperability more on the exchange carriers vice the DoD. Regardless, the problems associated with the deployment of ISDN over the years can certainly infiltrate the evolution of the DISN. For that reason, the various B-ISDN trials (testing) announced by several operating companies in the United States and elsewhere could help minimize interoperability problems during the far-term DISN

implementation. In the interim, network level testing between switch manufacturers during the evolution of B-ISDN will limit the long term impacts of deployment and could accelerate its use.

C. AREAS RECOMMENDED FOR FURTHER RESEARCH

1. Federal Telecommunications System-2000 (FTS-2000)

FTS-2000 is a government-wide upgrade of the Federal Telecommunications System. The General Services Administration (GSA) is responsible for administering the program. FTS-2000 consists of two separate network--Network A supported by AT&T and Network B supported by U.S. Sprint. With FTS-2000, voice, data, and video transmission will be supported over a variety of physical media, including those supporting ISDN and packet-switched environments. Communications requirements for FTS-2000 are functionally similar to those referenced by GOSIP when the requirements intersect (X.25 and X.400) [Ref. 58:p. K-3]. It should be considered as a connectivity adjunct to GOSIP; particularly GOSIP "valued-added" services. FTS-2000 will be interoperable with DSN and DCTN. Since FTS-2000 is essentially ISDN, interfaces to the evolving DISN will require conformance testing.

2. Tactical ISDN

ISDN is not just limited to the traditional computing atmosphere but can also be used in a tactical environment. Rome Air Development Center (RADC) has sponsored Massachusetts Institute of Technology (MIT) Lincoln Laboratory to investigate the use of tactical ISDN technology. The study focuses on how to utilize ISDN features

to meet requirements for secure voice and data communications in a tactical environment. Additionally, in a report published by AT&T, under the auspices of DCEC, they address several applications where tactical ISDN may be useful within the MILDEPS [Ref. 36:p. 3-5]:

- Standard terminal interface and single connection for voice and data would simplify the moves and changes that are common in a tactical environment.
- Compatibility with TRI-TAC transmission equipment is needed for ISDN to be of any short term benefit. Need for ISDN/Digital Group Multiplexer (DGM) gateway (ISDN/Tactical Air Command gateway).
- Lower bit rate connections using ISDN-like protocols for limited bandwidth tactical scenarios.

Tactical ISDN uses beyond those listed will continue to evolve as the ISDN standards continue to mature. The use of a tactical BRI interface (and eventually PRI) for tactical systems can provide substantial throughput and reduce the amount of conventional bandwidth.

3. Security-Related Applications

SDNS is being developed within the framework of OSI security. It proposes to serve as the basis for protecting classified data as well as unclassified but sensitive, data in a wide range of applications. SDNS can be used in a number of networks. There are several security related applications for use by DoD [Ref. 36:p. 3-7]: (1) use of existing secure equipment on ISDN, (2) secure ISDN phone, (3) secure voice/data terminal, (4) secure slow scan video, (5) secure full motion video for PRI applications, and (6) secure G4 facsimile. GOSIP specifies that security services may be provided at

one or more layers 2, 3, 4, 6, and 7 whereas SDNS development is at layers 3, 4, and 7. Furthermore, GOSIP Version 2 offers limited security capabilities at the network layer but will provide enhancements in GOSIP Version 3. An analysis of terminal adapters or native encryption BRI devices is needed to ensure devices under development can support a secure C^3 environment.

4. ISDN Interoperability with Defense Data Network (DDN)

Data transmission within ISDN is accomplished through either X.25 packet switching or circuit switching. When packet switching is desired by ISDN subscribers, the connection is made in accordance with CCITT X.25. However, the ISDN subscribers who need a packet switched connection through DDN may experience a problem because the DDN X.25 interface is not full compatible with CCITT X.25. This issue is addressed in MIL-STD 188-194. The optimal design objective is to have interoperability between ISDN X.25 and DDN X.25. This would allow an ISDN switch to serve as a multi-function/consolidated node for the DCS. As such, it could perform as an access point for switched voice on the DSN or packet switched data on the DDN. This could have unlimited payback in terms of cost. It could lessen equipment cost (it becomes a multi-function switch), operating cost, and potentially reduced facilities cost.

5. Miscellaneous

There are several miscellaneous issues affecting the full-scale implementation or deployment of ISDN and likewise B-ISDN:

- CCITT ISDN standards often provide network-specific supplementary services. These services are implemented in switches differently by each vendor and

sometime combines functions within other layers of the protocol. Therefore, incompatibilities could exist at virtually any layer of the network. This problem is more pronounced at the Central Office in the PSTN or End Office in the DSN level.

- Another issue is that the DSN uses the associated signalling mode with the quasi-associated signalling mode as a back up for DSN SS7. PSTNs are using the non-associated signalling mode for SS7 transmission and controls for STP/SPs. The method of transmission, management, and operation and control of the signalling between the DSN and PSTNs are different. Hence, a gateway-type of function may be required at each point where DSN SS7 and PSTN SS7 interoperate.

- A third factor regards the user interface. Feedback from implementors indicate that the user interfaces to ISDN terminals are virtually non-existent, and that appropriate user-friendly interfaces had to be developed in order to facilitate an easy transition to ISDN.

- The flexibility of ISDN induces complexity. There are 22 parameters that can be set in configuring the options of the simplest ISDN user device.

- The use of the CLNS, which is provided by the CLNP, allows different GOSIP subnetworks to interconnect as transparent OSI network entities (e.g., X.25 and ISDN). For GOSIP end systems, CLNS is mandatory, whereas CONS is an optional service. The use of CONS over ISDN can improve efficiency, potentially reduce the overhead of CLNS/CLNP, and increase overall throughput to support the C^3. Further analysis should be made to determine the cost effectiveness of incorporating CONS over ISDN.

- Extensive research is needed before the full deployment of DISN or B-ISDN to address: (1) the feasibility of incorporating the mixture of technologies proposed by the DISN in light of limited standards, (2) the ability to test these new technologies, (3) impacts the DISN will have on the MILDEPS in its migration from the current architecture.

APPENDIX A. ACRONYMS

Acronym	*Definition*
ACSE	Association Control Service Element
ADP	Automated Data Processing
AFCSA	Air Force Communications and Computer Systems Architecture
AFNET	Air Force Integrated Telecommunications Network
AIPC	Army Information Processing Centers
ANSI	American National Standards Institute
ASIMS	Army Standard Information Management System
ASW	Anti-submarine Warfare
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
Bellcore	Bell Communications Research
B-ISDN	Broadband Integrated Services Digital Network
BITS	Base Information Transfer System
BRI	Basic Rate Interface
C^2	Command and Control
C^3	Command, Control, and Communications
C^4	Command, Control, Communications, and Computers
C^4I	Command, Control, Communications, Computers, and Intelligence
CCC	CINC Command Center
CCITT	International Consultative Committee for Telegraph and Telephone
CINC	Commander-In-Chief
CJCS	Chairman, Joint Chiefs of Staff
CLNP	Connectionless Network Protocol
CLNS	Connectionless Network Service
CLTP	Connectionless Transport Protocol
CLTS	Connectionless Transport Service
CONS	Connection-Oriented Network Service
COTP	Connection-Oriented Transport Protocol
COTS	Commercial-off-the-shelf
CPE	Customer Premise Equipment
CSL	Computer Systems Laboratory

CSMA/CD	Carrier Sense, Multiple Access with Collision Detection
CVBG	Carrier Battle Group
DCE	Data Circuit-terminating Equipment
DCS	Defense Communications System
DCTN	Defense Commercial Telecommunications Network
DDN	Defense Data Network
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DLA	Defense Logistics Agency
DLANET	Defense Logistics Agency Network
DQDB	Distributed Queue Dual Bus
DMS	Defense Message System
DOD	Department of Defense
DPI	Data Processing Installation
DSCS	Defense Satellite Communication System
DSN	Defense Switched Network
DS-0	Digital Signal-0 (64 kbps)
DS-1	Digital Signal-1 (1.544 Mbps)
DS-3	Digital Signal-3 (44.736 Mbps)
DTE	Data Terminal Equipment
EHF	Extremely High Frequency
ES	End System
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FLTCINC	Fleet Commander in Chief
FTAM	File Transfer Access and Management
FTP	File Transfer Protocol
FTS-2000	Federal Telephone System-2000
GLOBIXS	Global Information Exchange System
GOSIP	Government Open Systems Interconnection Profile
GOTS	Government Off-the-Shelf
HDLC	High-level data link control
HF	High Frequency
IA	Industry Agreement
ICOT	ISDN Conformance Test
IDN	Integrated Digital Network
IEEE	Institute of Electrical and Electronics Engineers
IGOSS	Industry Government Open System Specifications
IMA	Information Mission Area
IP	Internet Protocol
IS	Intermediate System

ISA	Information System Architecture
ISDN	Integrated Services Digital Network
ISDNP	Integrated Services Digital Network Profiles
ISO	International Organization for Standardization
ITA	Information Transfer Architecture
ITS	Information Transfer System
IVD	Integrated Voice/Data
IXC	Interexchange Carrier
JCS	Joint Chiefs of Staff
JITC	Joint Interoperability Test Center
JTF	Joint Task Force
Kbps	Kilobits per second
LAN	Local Area Network
LAPB	Link Access Procedure B
LAPD	Link Access Protocol D
MAC	Medium Access Control
MAN	Metropolitan Area Network
MAP	Manufacturing Automated Protocol
Mbps	Megabits per second
MHS	Message Handling System
MILDEPs	Military Departments
MILSATCOM	Military Satellite Communications
MOT	Means of Test
NAVIXS	Navy Information Transfer System
NAVNET	Navy Network
NCA	National Command Authority
NDI	Non-Developmental Items
NIST	National Institute of Standards and Technology
NIUF	North American ISDN Users' Forum
NMCS	National Military Command System
NRC	National Research Council
NT1	Network Termination 1
NT2	Network Termination 2
NVLAP	National Voluntary Laboratory Accreditation Program
ODA	Office Document Architecture
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
PABX	Private Automatic Branch Exchange
PCTR	Protocol Conformance Test Report
PICS	Protocol Implementation Conformance Statement
PLP	Packet Layer Protocol
PRI	Primary Rate Interface
PSN	Packet Switch Node

PSPDN	Public Switched Packet Data Network
PSTN	Public Switched Telephone System
PVC	Private Virtual Circuit
RBOCs	Regional Bell Operating Companies
RDIXS	Research and Development Information Exchange System
SCTR	System Conformance Test Report
SDNS	Secure Data Network Service
SEW	Space and Electronic Warfare
SEWC	Space and Electronic Warfare Commander
SHF	Super High Frequency
SIGINT	Signal Intelligence
SMDS	Switched Multi-megabit Data Service
SMT	Station Management
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SSP	Service Switching Point
SS7	Signalling System Number 7, U.S. version
SS#7	Signalling System Number 7, international version
STP	Signal Transfer Point
STU-III	Secure Telephone Unit III
TA	Terminal Adaptor
TADIXS	Tactical Data Information Exchange System
TCC	Tactical Command Center
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TOP	Technical Office Protocol
TP	Transfer Protocol
TRI-TAC	Tri-Service Tactical
UHF	Ultra High Frequency
USAISEC	U.S. Army Information System Engineering Command
USCINC	U.S. Commander-In-Chief
VHF	Very High Frequency
VPN	Virtual Private Network
VT	Virtual Terminal
WAN	Wide Area Network
WWMCCS	Worldwide Military Command and Control System

APPENDIX B. JCS SM-684-88 DEFINED C3 ARCHITECTURES

1. System Architecture. A conceptual framework that includes operational concepts, capabilities, information flow, and connectivity (doctrinal utilization) of a C^3 system. Examples of this type architecture are the MILSATCOM and Secure Voice System architectures. System architectures are developed by the Service or Defense agencies for those systems under purview.

2. Mission Area Architectures. A framework for the evolution to future designs for the integrated C^3 systems, procedures, and support required to accomplish a specific mission or attain specific C^3 system characteristics. Mission area architectures incorporate system architectures. Functional Interoperability Architectures developed and managed by JIEO and intelligence communications architectures developed by the INCA Project Office are examples of this type architecture.

3. Subordinate or Component Command Architecture. Provides a conceptual framework of C^3 systems, procedures, and support for a subordinate or component command area of responsibility (AOR). The Alaskan Command C^3 architecture being developed by DISA/C4S and JIEO is an example of this type of architecture.

4. Theater Architecture. Provides a framework of C^3 systems, procedures, and support within a CINC's AOR evolving into target systems. It incorporates all the proceeding types of architectures. Examples are CINC interoperability architectures developed by JIEO and theater architectures developed by DISA/C4S facilities but can also include mobile C^3 capabilities.

5. NMCS Architecture. Provides the framework for the evolution of the current NMCS to future configurations in support of the NCA. While there is no evidence that a NMCS architecture exists, the Strategic C^3 System Description provides connectivity information on many of the systems which support strategic or non-strategic nuclear forces.

6. Service Architecture. The service architecture usually describes the overall objective C^3 system toward which a service is building. Examples are the Navy Copernicus architecture and the Army's Tactical Command and Control System (ATCCS). The mission area architecture incorporate system architectures, which are developed by the various services.

APPENDIX C. MAJOR STANDARDS-DEVELOPMENT ORGANIZATIONS

a. International Organization for Standardization (ISO): As early as 1976, the severity of the interoperability problem and the inability of proprietary network architecture to resolve it, was internationally recognized [Ref. 17:p. 6]. Committee work in the international standards community began to develop a methodology for solving the problem of communications between arbitrary systems in a multiple vendor environment. The purpose of ISO is to promote the development of standardization and related activities to facilitate international exchange of goods and services and to develop cooperation in the sphere of intellectual, scientific, technological, and economic activity [Ref. 18:p. 23]. OSI is designed to implement a common set of conventions for computer communications and computer networking. These standards provide a high level of confidence that systems on disparate networks will have a high probability of interoperability. Although ISO is not a governmental body, more than 70 percent of ISO member bodies are governmental standards institutions or organizations incorporated by public law. The member body for the United States is the American National Standards Institute (ANSI).

b. American National Standards Institute (ANSI). ANSI is a nonprofit, nongovernment federation of standards-making and standards-using organizations. Its

members include professional societies, trade association, governmental and regulatory bodies, industrial companies, and consumer groups. ANSI is the national clearing house for voluntary standards in the United States and is also the U.S.-designated voting member of the ISO. [Ref. 18:p. 2].

c. International Telegraph and Telephone Consultative Committee (CCITT): A committee of the International Telecommunications Union (ITU), which is itself a United Nations treaty organization. Hence the members of CCITT are governments. The U.S. representation is housed in the Department of State. The charter of CCITT is "to study and issue recommendations on technical, operating, and tariff questions relating to telegraphy and telephony." Its primary objective is to standardize, to the extent necessary, techniques and operations in telecommunication connections, regardless of the countries of origin and destination. [Ref. 19:p. 8].

d. National Institute of Standards and Technology (NIST): NIST is member of the Department of Commerce. Formerly called the National Bureau of Standards (NBS) until 1988, they issue Federal Information Processing Standards (FIPS) for equipment sold to the federal government. The concerns of NIST are broad, encompassing the areas of interest of both CCITT and ISO. NIST is attempting to satisfy federal government requirements with standards that, as far as possible, are compatible with international standards [Ref. 18:p. 2].

e. **Electronics Industries Association (EIA):** The EIA is a trade association of electronics firms and a member of ANSI. It is concerned primarily with standards that fit into OSI layer 1 (physical layer) [Ref. 18:p. 2].

f. **Institute of Electrical and Electronics Engineers (IEEE):** A professional society and a member of ANSI. Their concerns have primarily been with the lowest two layers of the OSI model (physical and data link layers) [Ref. 18:p. 2].

g. **North American ISDN Users' Forum:** The NIU-Forum was formed in 1987 by a group of government and industry representatives to encourage development of ISDN in the US and North America. It was conceived by NIST to address the national interest issues related to the upgrading of communications capabilities [Ref. 4:p. 7]. It is the voice in the implementation of ISDN and ISDN applications and helps to ensure that the emerging environment meets users' application needs. The primary output of the NIU-Forum is industry implementor agreements to produce interoperable products based on technical standards and options documented by the NIU-Forum. The actual work of the NIU-Form is accomplished by two workshops; the ISDN Users' Workshop (IUW) and the ISDN Implementors' Workshop (IIW).

(1) The IUW is responsible for identifying, defining, and prioritizing user requirements, as well as working with the IIW to define and approve agreements necessary to support the implementation of user requirements. Their efforts are designed

to identify potential user applications and structuring the IIW work to satisfy these applications. [Ref. 30:p. 1-3]

(2) The IIW is the technical arm of the NIU-Forum. Among their responsibility to develop application profiles and other agreements, the IIW is also has responsibility for developing conformance criteria. They offer technical advice and consultation to the IUW, sponsors multi-vendor demonstrations and trials, and provides formal liaisons with organizations such as COS, OSI Implementors' Workshop (OIW) or the ANSI T1 Committee. [Ref. 30:p. 1-3]

h. **Defense Information Systems Agency (DISA).** Formerly called the Defense Communications Agency (DCA), DISA promulgates communications-related military standards (MIL-STD). They are responsible for providing architectural guidance for national, joint, and combined C^3 systems. DoD feels that its requirements in some areas are unique, and this is reflected in standards that are unlike those used elsewhere [Ref. 18:p. 2]. DISA works closely with NIST and attempts to have military requirements satisfied by broader-based standards.

APPENDIX D. OSI REFERENCE MODEL LAYERS

1. Physical Layer

The physical layer is the bottom most level of the OSI Reference Model. It describes the electrical, mechanical, functional and procedural characteristics of communications between a DTE and a data circuit-terminating equipment (DCE). The general purpose interface between the DTE and DCE at the physical layer is CCITT X.21. The physical layer is responsible for transmitting and receiving bits of data over a transmission medium. Some of the most recognized interface standards associated with this layer include EIA-232-D, EIA-530, and the ISDN physical interface. The most common physical interface connection for ISDN is an 8-pin jack (RJ-4) much like the junction used to connect home telephones (RJ-11).

2. Data Link Layer

The data link layer, the second level, provides for reliable transfer of data across layer 1. It provides a means necessary to activate, maintain, and deactivate the link. The data link layer sends blocks of data (frames) with the necessary synchronization, error control, and flow control. With a fully functional data link protocol, the next higher layer may assume virtually error-free transmission. High-Level Data Link Control (HDLC), Link Access Protocol-Balanced (LAP-B), Logical Link

Control (LLC), and Link Access Procedure-D (LAP-D) are a few of the link standards associated with this layer.

3. Network Layer

The basic service of the network layer is for the transparent transfer of data between transport entities (or applications). This layer is responsible for establishing, maintaining, and terminating connections across communications facilities. The principle dialogue is between the station device and its nodes; the station sends addressed packets to the node for delivery across the network. Each device requests a virtual circuit connection, uses the connection to transmit data, and terminates the connection. The most common standards at this layer include CCITT's X.25 Packet Layer Protocol (PLP) and I.451 (common channel signalling).

4. Transport Layer

The fourth layer of the reference model is called the transport layer. This layer provides reliable, transparent transfer of data between end points with end-to-end error recovery and flow control. The purpose of layer 4 is to provide a reliable mechanism for the exchange of data between processes in different systems. The transport layer ensures that data packets are delivered error-free, in sequence, with no losses or duplications. The size and complexity of a transport protocol depends on the type of service it gets from the network layer below it. When a reliable layer 3 network layer (e.g., virtual circuit capability), a minimal transport layer is required. However,

if layer 3 is unreliable and/or only supports datagrams the layer 4 protocol should include extensive error detection and recovery [Ref. 18:p. 44]. Within the DoD protocol architecture, TCP provides this reliable service.

5. Session Layer

The purpose of the session layer is to provide the means for cooperating presentation entities to organize and synchronize their dialogue and to manage a variety of the data exchange services [Ref. 19:p. 216]. This layer is concerned with defining a variety of data exchange services that might be useful to applications. It provides a control mechanism for the exchange of information between applications and establishes, manages, and terminates sessions between user applications.

6. Presentation Layer

The presentation layer manages the display, exchange, and the data structure from application objects. It assures that end systems successfully communicate even if they use different representations. It also provides a common representation to be used in communication and converts data from a local representation to a common presentation.

7. Application Layer

This layer represents the top most layer of the OSI model. The application layer supports services such as electronic mail, file transfer between applications,

network management, transaction processing and more. These services, however, lie outside the seven-layer model. This layer contains management functions and generally useful mechanisms to support such distributed applications.

LIST OF REFERENCES

1. The Chairman Joint Chiefs of Staff Letter, CM-1127-91, Washington, DC, Subject: C2 Functional Analysis and Consolidation Review Panel Report, 2 November 1991.

2. Baldo, James and Levan, David O., *The Effects of Transition From DoD to OSI Communication Protocol,* Institute for Defense Analyses, IDA Paper P-2041, November 1987.

3. Beam, Walter R., *Command, Control, and Communications Systems Engineering,* McGraw-Hill Publishing Company, 1989.

4. Jacobovits, Mayer M., "A Conceptual Framework and Development Methodology for C3 Architecture", *Signal,* January 1989.

5. Balderman, M., LTC, C3 Architecture Review (J6E, J-6 Information Paper) 6 May 1991.

6. Fu, Y.S., Tate, T. Maj. and Hawrylko, W.P., "Evolution to a Broadband Defense Information Systems Network," paper presented at the 1991 IEEE Military Communications Conference (MILCOM 91), McLean, Virginia, November 5-7, 1991.

7. Department of the Navy, OP-094, *The Copernicus Architecture, Phase I: Requirements Definition,* August 1991.

8. Shultz, Beth, "Inverse Muxes Can Cut Costs," *Communications Week,* March 9, 1992.

9. Telephone conversation between Maj Tim A. Tate, DISA/DISN, Arlington, Virginia, and the author, 29 May 1992.

10. Brewin, Bob and Duffy-Marsan, Carolyn, "Pentagon OKs User-to-User Global Net", *Federal Computer Weekly,* March 16, 1992.

11. *Air Force Pamphlet (AFP) 700-50, Air Force Communications and Computer Systems Architecture Information Transfer Architecture (Draft),* Volume IV, December 1991.

12. Copernicus Project Team, "Copernicus Architecture," Space and Electronic Warfare (OP-094), Washington, DC.

13. U.S. Army Information Systems Command, *Information Systems Management Mission Area, Information Systems Architecture Overview,* Volume I, 1 November 1989.

14. Bauer, Dennis, and others, *Army Installation-Level Information Transfer System Assessment (Final)*, 9 March 1992.

15. USAISC, *Strategic and Sustaining Base Architecture, Information System Architecture, Technology and Standards,* Volume II, December 1991.

16. U.S. Department of Commerce, National Institute of Standards and Technology, *Government Open Systems Interconnection Profile Users' Guide,* Version 2, NIST Special Publication 500-192, Government Printing Office, Washington, DC, 1991.

17. Lini, Kenneth F., and Moore Joyce Y., *GOSIP Made Easy, The Complete Procurement Guide,* The Corporation for Open Systems International, 1990.

18. Stallings, William, *Data and Computer Communications,* 3d ed., Macmillan Publishing Company, 1991.

19. Stallings, William, *Handbook of Computer-Communications Standards, Department of Defense (DoD) Protocol Standards,* Volume 3, Macmillan Publishing Company, 1988.

20. The MITRE Corporation, *The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy*, May 1988.

21. U.S. Department of Commerce, National Institute of Standards and Technology, *Government Open Systems Interconnection Profile (GOSIP), Federal Information Processing Standard Publication 146-1,* U.S. Government Printing Office, Washington, DC, 1991.

22. Stallings, William, *Handbook of Computer-Communications Standards, The Open Systems Interconnection (OSI) Model and OSI-Related Standards,* Volume 1, Howard W. Sams and Company, 1987.

23. U.S. Department of Commerce, National Bureau of Standards, *Government Open Systems Interconnection Profile (GOSIP), Federal Information Processing Standard Publication 146,* National Technical Information Service, Springfield, Virginia, 1988.

24. Kuhn, Klaus, "NATO Policy and Transition Strategy for the Military Application of the ISO/CCITT Reference Model and its Associated Standards for Open System Interconnection," The Upper Layers of Open Systems Interconnection, paper presented at the Proceedings of the Second International Symposium on Interoperability of ADP Systems, The Hague, The Netherlands, 2-29 March 1985.

25. Stallings, William, *ISDN an Introduction,* Macmillan Publishing Company, 1989.

26. Kuehn, P.J., *ISDN-Technology, Networking Concepts and Applications,* Lecture Notes in Computer Science, Proceedings, Vol 248, paper presented at the Networking In Open Systems International Seminar, Oberlech, Austria, August 18-22, 1986.

27. National Institute of Standards and Technology Notices, *A Proposed Federal Information Processing Standard for Integrated Services Digital Network (ISDN),* Federal Register, Vol 7, No 8, January 13, 1992.

28. Defense Information Systems Agency, *Military Standard Integrated Services Digital Network Profiles (ISDNP),* MIL-STD-188-194, 1 November 1991.

29. Mier, Edwin E., "ISDN's Future: 2B or Not 2B," *Communications Week,* February 24, 1992.

30. U.S. Department of Commerce, National Institute of Standards and Technology, *North American ISDN Users' Forum Agreements on Integrated Services Digital Network*, NIST Special Publication 500-195, Government Printing Office, Washington, DC, 1991.

31. U.S. Department of Commerce, National Institute of Standards and Technology, *Stable Implementation Agreements for Open Systems Interconnection Protocols,* Version 4, Edition 1, NIST Special Publication 500-183, Government Printing Office, Washington DC, 1990.

32. Boisseau, Marc, *Telecommunications Trends In Europe,* Lecture Notes in Computer Science, Proceedings, Vol 248, paper presented at the Networking In Open Systems International Seminar, Oberlech, Austria, August 18-22, 1986.

33. Page, Bruce, "SS7 Networks, Why All The Sour Notes?," Network Testing Supplement, *Communications Week,* November 11, 1991.

34. Briere, Daniel, "Carriers Strive to Make ISDN More Visible," Network World, November 11, 1991.

35. Valovic, Thomas S., "Nationwide ISDN: One Step Closer to Reality?," *Telecommunications,* April 1991.

36. AT&T Federal Systems, *DCEC ISDN Application Evaluation, Task 2 Examination of Related ISDN Activities,* November 1991.

37. Walters, Stephen M., "A New Direction for Broadband ISDN," *IEEE Communications Magazine,* September 1991.

38. Lombardo, Nicholas, "Routers May Test Frame Relay Users' Patience," *Network World,* May 2, 1992.

39. Bingham, Sanford, Network Testing, "All the Right Moves, Jumping the Standards Track," *Communications Week,* November 11, 1991.

40. Netrix, *The Buyer's Guide to Frame Relay Networking,* 2d ed., Netrix Systems Corporation, 1991.

41. Gratzer, Frank, *Switched Multi-megabit Data Service,* Bell Communications Research, Bellcore Working Paper, No 1179-31.

42. McRoberts and Hemrick, *A Public-Network Data Service With The Look of A LAN,* Bellcore Exchange, January/February 1989.

43. Gareiss, Robin, "Sprint's Plan: SMDS Over Frame-Relay," *Communications Week,* February 24, 1992.

44. Zerbiec, T., "Considering the Past and Anticipating the Future for Private Data Networks," *IEEE Communications Magazine,* March 1992.

45. Healy, Eileen M., "SONET Overview and Standards Status," paper presented at the IEEE SONET Symposium, Middletown, New Jersey, November 1-16, 1989.

46. Norem, Dave, "North American ISDN User Forum, Long Range Plan," paper presented at the North American ISDN User's Forum Committee on ISDN Versions, 26-28 February 1991.

47. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Computer Systems Laboratory, Annual Report 1991,* NISTIR 4795, December 1991.

48. Mercier, Ann M., "DoD Unit to Handle GOSIP Testing," *Federal Computer Weekly,* December 2, 1991.

49. *Command, Control, Communications and Computers (and Intelligence) for the Warrior,* Joint Staff/J-6 Concept Paper, Undated (Approximately February 1992).

50. Telephone conversation between Mr. Dick Savoye, DISA/JIEO/TBBG, Reston, Virginia, and the author, 6 April 1992.

51. Technology Integration Center, Technical Strategies Branch (TIC/TINT), Scott Air Force Base, Illinois, *U.S. Air Force Government Open Systems Interconnect Profile (GOSIP) Transition Plan,* December 1991.

52. Telephone conversation between Mr. Timothy C. Bell, USAISC-MICOM, Redstone Arsenal, Alabama, and the author, 18 May 1992.

53. U.S. Department of Commerce, National Institute of Standards and Technology, *GOSIP Conformance and Interoperation Testing and Registration, Version 1.0,* NISTIR 4594, Government Printing Office, Washington, DC, 1991.

54. Powell, Dave, "When the Public Network Dies," *Network Management,* November 1991.

55. U.S. Department of Commerce, National Institute of Standards and Technology, *Trial of Open Systems Interconnection (OSI) Protocols Over Integrated Services Digital Network (ISDN),* NISTIR 89-4160, August 1989.

56. Greenstein, Irwin, "Capitalizing on ISDN Supply and Demand," *Network Management,* April 1992.

57. Defense Communications Engineering Center, DISA, *Network Engineering Plan for the Defense Information Systems Network,* July 11, 1991.

58. IMA, *Army Open Systems Interconnection (OSI) Interoperability and Transition Plan*, January 1990.

BIBLIOGRAPHIES

American National Standard for Telecommunications, *Integrated Services Digital Network (ISDN)-Minimal Set of Bearer Services for the Basic Rate Interface,* ANSI T1.604-1990, American National Standards Institute, 1990.

American National Standard for Telecommunications, *Integrated Services Digital Network (ISDN)-Minimal Set of Bearer Services for the Primary Rate Interface,* ANSI T1.603-1990, American National Standards Institute, 1990.

Bellcore, *Switched Multi-Megabit Data Service,* Digest of Technical Information, Issue 12, March 1988.

Burgin, John and Dorman, Dennis, "Network Management, Broadband ISDN Resource Management: The Role of Virtual Paths," *IEEE Communications,* September 1991.

Caston, Art, "Are Open Systems Coming of Age?", *Signal,* January 1989.

Defense Communications Agency, DCEC/R130, Subject: Common Format and Content of Individual Military Department and Defense Agency OSI Interoperability and Transition Plans, 31 January 1989.

Defense Communications Agency, *Military Standard Internet Protocol, MIL-STD-1777,* August 12, 1983.

Defense Communications Agency, *Military Standard Transmission Control Protocol, MIL-STD-1778,* August 12, 1983.

Defense Communications Agency, *Military Standard File Transfer Protocol, MIL-STD-1780,* May 10, 1984.

Defense Communications Agency, *Military Standard Simple Mail Transfer Protocol, MIL-STD-1781,* May 10, 1984.

Defense Communications Agency, *Military Standard Telnet Protocol, MIL-STD-1782,* August 12, 1983.

Endoso, Joyce, "Joint Chiefs Call for Open Systems in C^4I Blueprint," *Government Computer News,* March 2, 1992.

Henshall, John and Shaw, Sandy, *OSI Explained, End-to-End Computer Communication Standards,* Ellis Horwood Limited, 1988.

Herman, Edith, "Big Hurdle for SMDS," *Communications Week,* October 28, 1991.

Killette, Katheleen, "Getting Ready to Deploy National ISDN-1 Specifications", *Communications Week,* 24 February 1992.

Palmer, Dan L., "Unleashing SMDS," *Network Management,* August 1991.

Rose, Marshall T., *The Open Book, A Practical Perspective on OSI,* Prentice Hall, 1990.

Shantz, John, "SMDS: An Alternative to Private Networks?," *Telecommunications,* May 1989.

Stallings, William, *Handbook of Computer-Communications Standards, Local Network Standards,* Volume 2, Macmillan Publishing Company, 1987.

Technology Integration Center (AFCC)/TISC Letter, Scott Air Force Base, Illinois, Subject: Air Force Representative's Report of the North American ISDN User's Forum Committee on ISDN Versions (26-28 Feb 91).

The Joint Staff Letter, J-6A 00771-91, Washington, DC, Subject: Policy Direction for C3 Architectures, 1 May 1991.

Thyfault, Mary E., "LAN Interconnection, GSA Makes Pioneering Move," *Information Week,* Issue 373, May 11, 1992.

USAISC, *Information System Architecture,* Technology and Standards, Volume III, December 1991.

The Under Secretary of Defense C3I, *DoD Policy on Defense Data Network (DDN) Protocols,* 14 May 84.

U.S. Department of Commerce, National Institute of Standards and Technology, *ISDN Conformance Testing, Layer 1-Physical Layer, Part 1-Basic Rate S/T Interface, User Side,* NIST Special Publication 500-194, U.S. Government Printing Office, Washington, DC, 1991.

Wickham, John A., Jr., General, USA (Ret), "Desert Storm and the High Technology Debate," *Signal,* March 1991.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   Cameron Station
   Alexandria, Virginia 22304-6145

2. Library, Code 52 2
   Naval Postgraduate School
   Monterey, California 93943-5002

3. Joint Chiefs of Staff 1
   Attn: J6T, Room 1D826 (Lt Col G. Hollister)
   Pentagon, Washington, DC 20318-6000

4. AFIT/CIRK 1
   Wright-Patterson AFB, Ohio 45433

5. DISA/DISN 1
   Attn: Maj T.A. Tate
   Jefferson Building
   701 South Courthouse Road
   Arlington, Virginia 22204-2199

6. DISA/JIEO 1
   CFE/DRFB/Mr. M. DeFrancesco
   1860 Wiehle Avenue
   Reston, Virginia 22090-5500

7. DISA/JIEO/TBBG/R. Savoye 1
   11440 Isaac Newton Square, N
   Reston, Virginia 22090-5006

8. TIC/TIAA 1
   Building 1700
   Scott AFB, Illinois 62225-6343

9. TIC/TIAA 1
Building 1700
Scott AFB, Illinois 62225-6343

10. USAISC 1
Attn: ASQB-OSI-S (J. Thelander)
Fort Huachuca, Arizona 85613-6000

11. Naval Computer and Telecommunications Command 1
Computer and Communications Architecture Division, Code N50B
Bldg 19, Room 302E (Marthann McTighe)
4401 Massachusetts Ave, NW
Washington, DC 20394-5069

12. SM-ALC/LH 1
Attn: Col Leonard
McClellan AFB, California 95652

13. SM-ALC/LHCCM 1
McClellan AFB, California

14. Dr. Carl Jones, Code CC 1
Naval Postgraduate School
Monterey, California 93943-5002

15. Dr. Y.S. Fu, Code CC/FU 1
Naval Postgraduate School
Monterey, California 93943-5002

16. Dr. Myung Suh, Code AS/SU 1
Naval Postgraduate School
Monterey, California 93943-5002

17. Dr. Michael G. Sovereign, Code OR/SM 1
Naval Postgraduate School
Monterey, California 93943-5002

18. Captain Wayne R. Martin 1
102 Herrill Court
Folsom, California 95630

Thesis
M3589 Martin
c.1 C^3 interoperability
issues.

DUDLEY KNOX LIBRARY
3 2768 00018388 3